ELSTER

Customized Baustein CB 4.90 Loadbalancer

Version 1.2

27.03.2009

secunet
secunet Security Networks AG

Inhaltsverzeichnis

Inhaltsverzeichnis 2

Dokumentenhistorie 3

1 Einleitung 4

2 Baustein CB 4.90 Loadbalancer 5

2.1 Beschreibung 5

2.2 Gefährdungslage 6

2.2.1 Höhere Gewalt 6
2.2.2 Organisatorische Mängel 7
2.2.3 Menschliche Fehlhandlungen 11
2.2.4 Technisches Versagen 13
2.2.5 Vorsätzliche Handlungen: 15

2.3 Maßnahmenempfehlungen 19

2.3.1 Planung und Konzeption 19
2.3.2 Beschaffung 24
2.3.3 Umsetzung 26
2.3.4 Betrieb 38
2.3.5 Aussonderung 57
2.3.6 Notfallvorsorge 63

3 Kreuzreferenztabellen 69

Dokumentenhistorie

Version	Änderung	Datum	Autor
0.1	Initiale Erstellung	24.05.2007	U. Kersten
0.2	Diverse Korrekturen	06.06.2007	U. Kersten
0.5	Review und Überarbeitung	19.06.2007	R. Lipowsky
1.0	Review und Freigabe durch PL	19.12.2007	R. Lipowsky
1.1	Überarbeitung/Korrektur von Inkonsistenzen	18.01.2008	R. Lipowsky
1.2	Ergänzungen der Gefährdungen G 2.54, G 5.112, G 5.113 lt. Auditbericht Plan42 v. 14.03.2008	28.03.2008	M. Gebauer

1 Einleitung

Ein vorgefertigter Baustein für Loadbalancer existiert nicht im Rahmen des GSHB des BSI, ist aber oft zur vollständigen Modellierung vieler IT-Verbünde notwendig. Das GSHB erlaubt bzw. fordert für Nicht-Standard-Anwendungen und -Systeme die Erstellung eines angepassten oder neuen Bausteins mit den relevanten Gefährdungen und den daraus resultierenden Sicherungsmaßnahmen.

Dieser Baustein für Loadbalancer wurde auf Basis des Bausteines B 3.302 Router und Switches, B 3.101 Allgemeine Server und B 3.301 Sicherheitsgateway unter Zuhilfenahme der Standardmaßnahmen des GSHB erstellt.

Dabei wurden die Original-Gefährdungen des GSHB an die Bedingungen von Loadbalancer angepasst, ihre Nummerierung jedoch nicht verändert. Um die Veränderung zu kennzeichnen wurden ihre Bezeichner mit einem Stern versehen.

Angepasste Maßnahmen (in denen der ursprüngliche Wortlaut der im GSHB enthaltenen Maßnahmen verändert wurde) erhielten ebenfalls einen mit einem Stern gekennzeichneten Bezeichner. Da die Inhalte der jeweiligen Maßnahmen meist generisch aufgebaut sind, wurden sie, wenn immer möglich, sinngemäß übernommen und auf die Gegebenheiten von Loadbalancern übertragen.

2 Baustein CB 4.90 Loadbalancer

2.1 Beschreibung

Ein Loadbalancer ist ein Gerät, das in der Lage ist, eine große Anzahl von Zugriffen über dedizierte TCP- oder UDP-Ports bzw. IP-Protokolle auf zwei oder mehrere Server zu verteilen. Dadurch werden folgende Effekte erzielt:

- Der Ausfall eines Servers durch Wartungsarbeiten oder technisches Versagen führt nicht zum Gesamtausfall des angebotenen Dienstes.
- Das zeitliche Antwortverhalten für die angebotenen Dienste verbessert sich.
- Die Dimensionierung der Serversysteme kann so gewählt werden, dass an Stelle eines großen (teuren) Systems mehrere kleine und damit kostengünstigere Server eingesetzt werden können. Außerdem wird eine bessere Skalierbarkeit des Gesamtsystems erreicht.
- Es können für den Fall, dass das Maximum an zulässigen Verbindungen für einen Server überschritten wird, so genannt Overflow-Server definiert werden, welche dann die zusätzlichen Verbindungen für diesen Service annehmen.
- Es können auch Informationen aus der Anwendungs-Schicht des OSI-Modells bzw. der Datenteil der IP-Pakete ausgewertet werden, die für eine weitergehende Art der Lastverteilung herangezogen werden (z.B. die Art des angeforderten Contents).

Loadbalancer wurden ursprünglich aus der Erkenntnis heraus entwickelt, dass die Intelligenz, die in den GigabitEthernet Controllern schon integriert war, dazu benutzt werden konnte, um sogenannte Sitzungstabellen zu generieren und zu halten. Diese stellen die Basis für das Loadbalancing dar. Deshalb waren frühe Modelle der Loadbalancer Chassis-basierte Geräte mit mehreren GigabitEthernet Interfacekarten und einen zusätzlichen Controllermodul, das für die Konfiguration und Administration benutzt wurde. Dieser Ansatz ist heute noch im Linux-Umfeld anzutreffen, wo entsprechende Projekte existieren, die oft von einer Appliance mit mehreren NIC´s als Grundlage ausgehen.

In einen anderen Entwicklungszweig haben sich die so genannten Hardware-Loadbalancer etabliert, die auf hochintegrierten Asics beruhen und häufig Multiprozessorsysteme mit einem speziellen Echtzeit-Betriebssystem darstellen. Sie können neben dem normalen Layer-2 Switching auch meist mit VLAN-Informationen umgehen (IEEE 802.1q) und beherrschen sowohl Routing (statisches und/oder dynamisches) als auch IP-Adressumsetzung (NAT). Hinzu kommt noch die Filterfunktionalität, die bis Layer-4 Information verarbeiten und diverse Aktionen beinhalten kann.

Ein Loadbalancer kann an den unterschiedlichsten Stellen im Kommunikationsweg implementiert werden. Dies ermöglicht z. B. die folgenden Einsatzszenarien:

- Der Loadbalancer wird im Internet platziert, um z. B. als Bestandteil einer hochverfügbaren Firewall, als Teil der redundanten Anbindung eines Unternehmens über mehrere ISP´s oder als Bestandteil einer globalen Internetpräsenz zu dienen.
- Der Loadbalancer wird in der DMZ platziert, um z. B. als Bestandteil eines hochverfügbaren Web- oder FTP-Serversystems oder e-commerce-Plattform zu dienen. Die Benutzer greifen über das Internet und durch eine Firewall abgesichert auf die angebotenen Dienste zu. Die Administration erfolgt oft durch eine weitere Firewall abgesichert vom Intranet aus oder über ein separates Managementnetz.
- Der Loadbalancer wird im Intranet platziert, um z. B. als Bestandteil einer hochverfügbaren Datenbankplattform zu dienen. Die Benutzer greifen über das Internet und durch eine Firewall abgesichert auf die angebotenen Dienste zu.

Aus diesen Szenarien ergeben sich unterschiedliche Gefährdungen für den Einsatz und den Betrieb eines Loadbalancers, welche bei der Planung und Umsetzung von entsprechenden Maßnahmen berücksichtigt werden müssen.

2.2 Gefährdungslage

Aufgrund der Vielzahl an Funktionen und der Komplexität der Einsatzszenarien sind Loadbalancer einer Reihe von Gefährdungen ausgesetzt.

Für den IT-Grundschutz von Loadbalancer werden folgende typische Gefährdungen angenommen:

2.2.1 Höhere Gewalt

G 1.2*	**Ausfall des Loadbalancers** Der Ausfall des Loadbalancer kann zum Ausfall des gesamten IT-Betriebs führen. Als zentrale Komponente eines IT-Systems, über welche die lastverteilten Anwendungen geführt werden, ist sie geeignet, solche Ausfälle herbeizuführen.

2.2.2 Organisatorische Mängel

G 2.1*	**Fehlende oder unzureichende Regelungen** Übergreifende und organisatorische Regelungen und Vorgaben spielen eine wichtige Rolle auch für Loadbalancer. Die Regelungen umfassen z.B. die Festlegung der Zuständigkeiten für die Administration und Konfiguration des Loadbalancers, Zugriffsregeln auf den Loadbalancer usw. Fehlende oder unzureichende Regelungen können große Auswirkungen auf die Verfügbarkeit sowie die Sicherheit des Loadbalancer nach sich ziehen. Aber nicht nur fehlende oder unzureichende Regelungen haben negative Auswirkung auf den IT-Betrieb, sondern auch nicht angepasste Regelungen. Oft werden nach Veränderungen technischer, organisatorischer oder personeller Art, die wesentlichen Einfluss auf die IT-Sicherheit haben, bestehende Regelungen nicht angepasst. Veraltete Regelungen können dem störungsfreien IT-Betrieb entgegen stehen.
G 2.3 *	**Fehlende, ungeeignete, inkompatible Betriebsmittel** Eine nicht ausreichende Bereitstellung von Betriebsmitteln kann einen IT-Betrieb erheblich beeinträchtigen. Störungen können sich ergeben, weil benötigte Betriebsmittel nicht in ausreichender Menge vorhanden sind oder nicht termingerecht bereit gestellt wurden. Zum Beispiel kann die nicht termingerechte Bereitstellung eines Lizenz-Schlüssels, der für die Freischaltung einer speziellen Funktion gesondert bestellt und auf dem Loadbalancer eingespielt werden muss, die Realisierung einer IT-Maßnahme verzögern und so den Betrieb beeinträchtigen.
G 2.4	**Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen** Nach der Einführung von Maßnahmen, die der Sicherheit der IT dienen, müssen diese auch konsequent umgesetzt werden. Finden keine oder nur unzureichende Kontrollen der Sicherheitsmaßnahmen statt, wird weder deren Missachtung noch ihre effektive Wirksamkeit festgestellt. Eine rechtzeitige und der jeweiligen Situation angemessene Reaktion wird dadurch verhindert. Darüber hinaus gibt es Sicherheitsmaßnahmen, die nur mit der Durchführung entsprechender Kontrollen ihre Wirkung entfalten. Hierzu zählen beispielsweise Protokollierungsfunktionen, deren Sicherheitseigenschaften erst mit der Auswertung der Protokolldaten zum Tragen kommen.

G 2.22*	**Fehlende Auswertung von Protokolldaten** Die meisten Loadbalancer bieten Funktionalitäten an, um die Nutzung der Operationen, ihre Reihenfolge und ihre Auswirkungen zu protokollieren. Im Lebenszyklus eines Loadbalancers kommen verschiedene Protokollierungskonzepte zum Einsatz. Während der Einrichtungsphase werden ausführliche Protokolle genutzt, um im Fehlerfall die Protokolldaten für eine detaillierte Problemanalyse heranziehen zu können und die Fehlerbehebung zu erleichtern. In der Einführungsphase werden Protokolle genutzt, um unter anderem die Performance des Loadbalancers in der Produktivumgebung zu optimieren oder um die Wirksamkeit des Sicherheitskonzepts erstmals in der Praxis zu überprüfen. In der Produktivphase werden Protokolle hauptsächlich auf die Sicherstellung des ordnungsgemäßen Betriebs bezogen. Protokolldaten dienen dann dem Zweck, nachträglich feststellen zu können, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein Angriffsversuch unternommen wurde. Protokolldaten werden für die Fehleranalyse im Schadensfall und zur Ursachenermittlung bzw. zur Integritätsprüfung genutzt. Die Protokollierung kann auch der Täterermittlung und damit auch der Abschreckung von potenziellen Tätern dienen. Durch regelmäßige Auswertung der Protokolldaten können vorsätzliche Angriffe auf ein IT-System unter Umständen frühzeitig erkannt werden. Findet die Auswertung der Protokolldaten nicht oder nur unzureichend statt, können diese nicht für Präventivmaßnahmen genutzt werden. Beispiel: Ein nicht autorisierter Benutzer versucht, Zugriff auf einen Loadbalancer zu erlangen, indem er zu bekannten Benutzernamen die entsprechenden Passwörter rät. Die erfolglosen Authentisierungsversuche werden im System protokolliert. Aufgrund fehlender Auswertung der Protokolldateien werden die Angriffsversuche nicht erkannt. Der unautorisierte Benutzer kann unerkannt den Angriffsversuch gegebenenfalls bis zum Erfolg fortsetzen.
G 2.27 *	**Fehlende oder unzureichende Dokumentation** Verschiedene Formen der Dokumentation können betrachtet werden: die Produktbeschreibung, die Administrator- und Benutzerdokumentation zur Anwendung des Produktes und die Systemdokumentation. Eine fehlende oder unzureichende Dokumentation der eingesetzten Loadbalancer kann sowohl im Auswahl- und Entscheidungsprozess für ein Produkt, als auch bei einem Schadensfall im Wirkbetrieb erhebliche Auswirkungen haben.

	Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. deren Fehlfunktion, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein. Dies gilt auch für die Dokumentation des Aufbaus und der Verkabelung von IT-Systemen, deren Funktion wesentlich von der korrekten Beschaltung des Laodbalancers abhängig ist (Client-Prozessing, Server-Prozessing).
G 2.44 *	**Inkompatible aktive und passive Netzkomponenten** Durch inkompatible aktive Netzkomponenten können Probleme verursacht werden, die im Umfeld nicht oder noch nicht vollständig standardisierter Kommunikationsverfahren auftreten. Um das betreffende Kommunikationsverfahren nutzen zu können, sind die Hersteller aufgrund der fehlenden oder nur teilweise vorhandenen Standards gezwungen, proprietäre Implementierungen einzusetzen. Inkompatibilitätsprobleme dieser Art können entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Hersteller ergänzt werden oder wenn Netze mit Netzkomponenten unterschiedlicher Hersteller aufgebaut werden. Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen des gleichen Kommunikationsverfahrens gemeinsam in einem Netz betrieben, kann es zu einem Verlust der Verfügbarkeit des gesamten Netzes, von einzelnen Teilbereichen oder bestimmter Dienste kommen (IEEE 802.1q vs. ISL). Aber auch die Kombination von inkompatiblen passiven Netzkomponenten kann die Verfügbarkeit eines Netzes gefährden. So existieren für Twisted-Pair-Kabel Ausführungen in 100 und 150 Ohm, die nicht ohne einen entsprechenden Umsetzer zusammen verwendet werden dürfen. Beispiel: Loadbalancer sind in der Regel mit Ports ausgestattet, die sich nur mit einer strukturierten Verkabelung nach EN 50173 betreiben lassen. Der Anschluss von Endgeräten über 50 Ohm Koaxialkabel ist nicht möglich.
G 2.54 *	**Vertraulichkeitsverlust durch Restinformationen** Bei elektronischer Datenübermittlung oder Datenträgerweitergabe passiert es immer wieder, dass dabei auch Informationen weitergegeben werden, die die Institution nicht verlassen sollten. Als mögliche Ursachen für die unbeabsichtigte Weitergabe von Informationen lassen sich folgende Beispiele anführen: • Restinformationen auf Datenträgern, Bei den meisten Dateisystemen werden Dateien, die vom Benutzer über einen Löschbefehl gelöscht werden, nicht wirklich in dem Sinn gelöscht, dass die Information an-

	schließend nicht mehr vorhanden ist. Normalerweise werden lediglich die Verweise auf die Datei aus den Verwaltungsinformationen des Dateisystems (etwa aus der Dateizuordnungstabelle (*File Allocation Table*) beim FAT-Dateisystem) gelöscht und die zu der Datei gehörenden Blöcke als "frei" markiert. Der tatsächliche Inhalt der Blöcke auf dem Datenträger bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden. • Wenn Datenträger an Dritte weitergegeben werden, beispielsweise o wenn ein Loadbalancer ausinventarisiert wurde und verkauft wird, o wenn ein defektes Gerät zur Reparatur gegeben oder im Rahmen der Garantie ausgetauscht wird oder o wenn ein Datenträger im Rahmen des Datenträgeraustauschs an einen Geschäftspartner weitergegeben wird können auf diese Weise sensitive Informationen nach draußen gelangen.
G 2.98 *	**Fehlerhafte Planung und Konzeption des Einsatzes von Loadbalancern** Bei der Planung des Einsatzes aktiver Netzkomponenten stehen meistens die Aspekte Funktionalität und Leistungsfähigkeit im Vordergrund. Wenn der Betrieb von Loadbalancer, als ein zentrales Element im Netz, nicht in das unternehmensweite Sicherheitskonzept eingebunden wird, kann der sichere Einsatz dieser Komponente nicht sichergestellt werden. Die Fehler bei der Planung des Einsatzes von Loadbalancern fallen meist in eine der folgenden Kategorien: <u>Unzureichende Berücksichtigung des Einsatzzwecks der Geräte</u> • Oft wird der Einsatzzweck der Komponenten bei der Planung nicht ausreichend berücksichtigt. Als Beispiel soll hier der Einsatz von VLANs genannt werden. Diese bieten keine Sicherheit bei der Trennung von Netzen, die eine Vielzahl von Angriffspunkten bieten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind • Auch bei der Planung des Einsatzes von Routing-Protokollen können Fehler gemacht werden. Wenn Loadbalancer im Bereich von demilitarisierten Zonen (DMZs) eingesetzt werden, kann die Verwendung von dynamischen Routing-Protokollen die Verfügbarkeit, Vertraulichkeit und die Integrität des zu schützenden Netzes gefährden. <u>Unzureichende Berücksichtigung von Sicherheitsmechanismen</u> • Es können beispielsweise zusätzliche Maßnahmen erforderlich werden, falls ein Gerät bestimmte Sicherheitsmechanismen nicht unterstützt. Wenn dies nicht bereits in der Planungsphase berücksichtigt wird, kann es später zu Problemen führen, wenn die Notwendigkeit

	erkannt wird. • Als Beispiel soll die Einrichtung eines gesonderten Administrationsnetzes (Out-of-Band Management)dienen. Falls die gewählten oder vorhandenen Geräte nur unsichere Protokolle wie SNMPv1, SNMPv2 oder Telnet unterstützen, so ist die Einrichtung eines Administrationsnetzes unbedingt erforderlich. Eine Nichtbeachtung dieser Fakten in der Planungsphase resultiert in Schwierigkeiten bei der Einrichtung des Administrationsnetzes, sofern der notwendige Anschluss nicht schon als separater Port vorhanden ist. Fehlende oder mangelhafte Information und Dokumentation Gelegentlich sind in der Planungsphase notwendige Informationen nicht vorhanden, da entweder keine entsprechende Dokumentation vom Anbieter zur Verfügung gestellt wurde oder die betreffenden Dokumente nicht berücksichtigt werden. Fehlentscheidungen, die auf Grund mangelhafter Dokumentation gemacht wurden, sind oft nur schwer zu korrigieren, wenn sich beispielsweise später herausstellt, dass ein Gerät bestimmte Funktionen nicht oder nur unzureichend unterstützt. Als Beispiele können die Unterstützung von SSH oder Radius zu Authentifizierung des Administrators dienen.

2.2.3 Menschliche Fehlhandlungen

G 3.64*	**Fehlerhafte Konfiguration von Loadbalancern** Die Konfiguration aktiver Netzkomponenten hängt stark vom Einsatzzweck der Geräte ab. Wenn der Betrieb von Loadbalancern nicht in das unternehmensweite Sicherheitskonzept eingebunden wird, kann der sichere Einsatz dieser Komponenten nicht sichergestellt werden. Nachfolgend sind einige Beispiele aufgeführt, die den sicheren Einsatz der Geräte bedrohen können. Betriebssystem Oft werden mit Loadbalancern veraltete oder unsichere Versionen von Betriebssystemen (Firmware) ausgeliefert und dann verwendet. Für eine Vielzahl von Versionsständen für Betriebssysteme unterschiedlicher Geräte und Hersteller stehen auf einschlägigen Seiten im Internet Exploits zum Angriff auf diese Geräte zum Download bereit. Passwortschutz Der Zugriff auf aktive Netzkomponenten wird oft nur unzureichend durch Passwörter geschützt bzw. es werden die vom Hersteller voreingestellten Logindaten weiterverwendet. Dies gilt auch für den Zugriff über den Konsolen-Port.

	Administrationszugänge Administrationszugänge sind in der Praxis oft frei zugänglich. Es sind beispielsweise keine Access Control Lists (ACL) eingerichtet, um den Kreis der möglichen Administratoren einzuschränken. Remote-Zugriff Aktive Netzkomponenten bieten in der Regel die Möglichkeit mit Hilfe von TELNET remote zuzugreifen. Bei der Nutzung von TELNET werden Benutzername und Passwort im Klartext übertragen. Login-Banner Login-Banner von aktiven Netzkomponenten verraten häufig die Modell- und Versionsnummer des Geräts. Schnittstellen Nicht genutzte Ports auf den aktiven Netzkomponenten sind häufig nicht deaktiviert. VLAN Trunk-Ports können auf alle konfigurierten VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs ermöglicht. Häufig sind auf Switches die Trunking-Protokolle auf den Endgeräte-Ports nicht deaktiviert. Siehe auch G 5.114 Überwindung der Grenzen zwischen VLANs. Routing-Protokolle Bei der Verwendung eines Loadbalancers als schneller Router ist die Auswahl des geeigneten Routing-Prokolls sehr wichtig. Routing-Protokolle ohne Authentisierungsverfahren können die Vertraulichkeit, Verfügbarkeit und Integrität komplexer Netze bedrohen.
G 3.65*	**Fehlerhafte Administration von Loadbalancern** Eine fehlerhafte Administration von Loadbalancern kann die Verfügbarkeit, Vertraulichkeit und Integrität von Netzen bedrohen. Es gibt unterschiedliche Zugriffsmöglichkeiten, um Loadbalancer zu administrieren, die bei falscher Anwendung ein Sicherheitsrisiko darstellen können: Remote-Administration Die Remote-Administration mit Hilfe des Dienstes Telnet, dessen Nutzung die Gefahr der unbefugte Erlangung von Zugriffsrechten birgt, da der Datenverkehr inklusive des Benutzernamens und Passwortes im Klartext mitgelesen werden kann. Die Remote-Administration mit Hilfe des Dienstes HTTP beruht darauf, dass auf dem Loadbalancer ein HTTP-Server gestartet ist, der Zugriff von beliebigen Clients über Web-Browser ermöglicht. Eine Gefährdung besteht dann, wenn die

	Nutzung dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen erfolgen kann. Wie bei der Nutzung des Dienstes Telnet werden auch beim HTTP der Benutzername und das Passwort im Klartext übertragen. Zudem ist eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server unterschiedlicher Hersteller ausnutzen. SNMP Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten "Community Strings". Als Standardeinstellung bei nahezu allen Herstellern ist der read-Community-String auf den Wert "public" eingestellt, während der write-Community-String auf den Wert "private" gesetzt ist. Die SNMP Community Strings werden im Klartext über das Netz übertragen. Oft wird SNMP über nicht abgesicherte Netze genutzt, so dass ein Angreifer in der Lage ist, durch Mitlesen der Datenpakete (Sniffen) SNMP Community Strings zu erraten. Nach Kenntnisnahme der Community Strings kann ein Angreifer die Kontrolle über den Loadbalancer übernehmen. Protokollierung Häufig werden sicherheitsrelevante Ereignisse auf Loadbalancer nur unzureichend protokolliert, weil bei der Einrichtung des Loadbalancers die Auditfunktionalität nicht aktiviert wurde. Zudem kann sich eine fehlende Alarmierungs-Komponente negativ auf die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme auswirken. Fehlendes Backup und Dokumentation Werden Konfigurationsänderungen auf Loadbalancern nicht gesichert und nicht dokumentiert, so stehen beim Ausfall der Komponenten die letzten Änderungen beim Wiederanlauf des Ersatzsystems nicht zu Verfügung.

2.2.4 Technisches Versagen

G 4.22*	**Software-Schwachstellen oder -Fehler** Wie für jede Software gilt auch für Loadbalancersoftware: je komplexer sie ist, desto häufiger treten Programmierfehler auf. Es ist zu beobachten, dass hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Erscheinungstermine auch dazu führen können, dass die Hersteller ihre Produkte nicht fehlerfrei anbieten. Werden diese Softwarefehler nicht erkannt, können die bei der Anwendung entstehenden Fehler zu weitreichenden Folgen führen. Beispiel: Das Übertragen einer großen Konfigurationsdatei per Kopieren und Einfügen innerhalb einer Telnet-Sitzung über einen Managementport führte bei einem

	Loadbalancer zu einem Systemabsturz. Die betroffene Firmwareversion musste von Hersteller modifiziert werden.
G 4.49 *	**Unsichere Default-Einstellung auf Loadbalancer** Aktive Netzkomponenten werden von Herstellern oft mit unsicheren Default-Konfigurationen ausgeliefert, die den sicheren Einsatz gefährden. Bei einigen Geräten zeigen außerdem die Systembefehle zur Anzeige einer Konfiguration nicht alle Parameter an. Folgende Aspekte sind häufig problematisch: Betriebssystem Aktive Netzkomponenten werden oft mit einem veralteten Versionsstand des Betriebssystems ausgeliefert. Hostname Werkmäßig eingestellte Hostnamen verraten oft den Hersteller der Geräte. Dienste Werkseitig werden Geräte mit Standardkonfigurationen ausgeliefert, auf denen eine Vielzahl von Diensten aktiviert sind. Beispielsweise können dies HTTP, Telnet, FINGER oder sonstige Dienste sein. Benutzerkonten und Passworte Werksmäßig eingerichtete Benutzerkonten haben dokumentierte und damit allgemein bekannte Standardnamen und -Passworte. Auf einschlägigen Internet-Seiten stehen Listen mit herstellerspezifischen Standard-Accounts und Passworten zum Download bereit. Unsichere SNMP-Versionen Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten sogenannten Community Strings. Als Standardeinstellung bei nahezu allen Herstellern ist der Read-Community-String auf den Wert "public" eingestellt, während der Write-Community-String auf den Wert "private" gesetzt ist. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden. Routing-Protokolle Auf Loadbalancer verschiedener Hersteller sind standardmäßig Routing-Protokolle aktiviert. Login-Banner Werksmäßig verraten Login-Banner unterschiedlicher Geräte beispielsweise die Modell- und Versionsnummer des Gerätes. Diese Angaben können für die

	gezielte Auswahl bekannter Exploits verwendet werden und erleichtern Angreifern so die Durchführung von Angriffen.

2.2.5 Vorsätzliche Handlungen:

G 5.4	**Diebstahl** Durch den Diebstahl von IT-Geräten, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und daraus resultierenden Konsequenzen entstehen.
G 5.28	**Verhinderung von Diensten** Ein solcher Angriff, auch "Denial of Service" genannt, zielt darauf ab, die IT-Benutzer daran zu hindern, Funktionen oder Geräte zu benutzen, die ihnen normalerweise zur Verfügung stehen. Es können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit Dies kann z. B. geschehen durch: • die gezielte Überlastung des Netzes (Syn-Flood, Smurf-Angriff) • das Kappen von Netzverbindungen.
G 5.112	**Manipulation von ARP-Tabellen** Im Gegensatz zu einem Hub kann bei einem Switch grundsätzlich die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen abgehört werden. Zu diesem Zweck pflegt der Switch eine Tabelle, die die MAC-Adressen der beteiligten Stationen den verschiedenen Ports zuordnet. Datenpakete beziehungsweise Ethernet-Frames, die an eine bestimmte MAC-Adresse adressiert sind, werden nur an den Port weitergeleitet, an dem der betreffende Rechner angeschlossen ist. Doch nicht nur der Switch pflegt eine Tabelle mit MAC-Adressen, sondern auch die beteiligten Rechner. Mit ARP-Anfragen können diese ARP-Tabellen am beteiligten Rechner gefüllt werden. Ziel des ARP-Spoofings ist es, die ARP-Tabellen zu manipulieren (ARP-Cache-Poisoning). Dazu schickt ein Angreifer eine ARP-Antwort an das Opfer, in der er seine eigene MAC-Adresse als die des Routers ausgibt, der für das betreffende Subnetz als Standard-Gateway fungiert. Sendet das Opfer anschließend ein Paket zum eingetragenen Standard-Gateway, landet dieses Paket in Wirklichkeit beim Angreifer. Auf dieselbe Weise wird der ARP-Cache des Routers so manipuliert, dass Ethernet-Frames, die eigentlich an das Opfer adressiert wurden, in

	Wirklichkeit beim Angreifer landen. Auf einschlägigen Internet-Seiten sind eine Reihe von Tools verfügbar, die diese Angriffsmethode ermöglichen. MAC-Flooding ist eine Angriffsmethode, die die Funktionsweise eines Switches beeinflusst. Switches erlernen angeschlossene MAC-Adressen dynamisch. Die MAC-Adressen werden in der Switching-Tabelle gespeichert. Der Switch weiß dadurch, an welchen Ports die entsprechenden MAC-Adressen angeschlossen sind. Wenn nun eine angeschlossene Station mit Hilfe eines geeigneten Tools eine Vielzahl von Paketen mit unterschiedlichen Quell-MAC-Adressen sendet, speichert der Switch diese MAC-Adressen in seiner Switching-Tabelle. Sobald der Speicherplatz für die Switching-Tabelle gefüllt ist, sendet ein Switch sämtliche Pakete an alle Switch-Ports. Durch dieses "Fluten" der Switching-Tabelle mit sinnlosen MAC-Adressen kann ein Switch nicht mehr feststellen, an welche Ports tatsächliche Ziel-MAC-Adressen angeschlossen sind. Diese Angriffsmethode wird verwendet, um das Mitlesen von Paketen in geswitchten Netzen zu ermöglichen. Es sind frei verfügbare Tools auf einschlägigen Seiten im Internet verfügbar, die auf einem Switch über 155.000 MAC-Adress-Einträge innerhalb einer Minute erzeugen können.
G 5.113	**MAC-Spoofing** Die MAC-Adresse ("media access control") eines Geräts ist eine vom Hersteller vorgegebene Adresse, mit der Geräte auf der OSI-Schicht 2 adressiert werden. Verschiedene Sicherungsmechanismen auf der Netzebene (beispielsweise Port-Security bei Switches) beruhen darauf, dass eine Verbindung nur von einem Gerät mit einer bestimmten MAC-Adresse aufgebaut werden darf. Mit Hilfe entsprechender Programme kann ein Angreifer die MAC-Adresse seines Gerätes ändern und Ethernet-Frames mit einer fremden Kennung in das Netzsegment schicken. Auf diese Weise können Sicherungsmechanismen umgangen werden, die allein auf der Verwendung einer MAC-Adresse beruhen. Der Angreifer muss sich dabei allerdings im selben Netzsegment befinden oder sogar Zugang zu demselben Switchport haben wie das Gerät, als das er sich mittels MAC-Spoofing ausgibt. Eine Gefährdung durch MAC-Spoofing besteht auch bei drahtlosen Netzen (WLAN), bei denen am Access-Point eine entsprechende Zugangskontrolle konfiguriert wurde.
G 5.114*	**Missbrauch von Spanning Tree** Das Spanning Tree Protokoll ist in IEEE 802.1d spezifiziert. Spanning Tree wird verwendet, um Schleifenbildungen innerhalb eines Netzes mit mehreren Switches zu vermeiden. Bei diesem Verfahren werden redundante Netzstrukturen ermittelt und in eine zyklenfreie Struktur abgebildet. Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzstruktur auf eine Baumstruktur.

	Da Spanning Tree keine Authentisierung beim Austausch von Bridge Protocol Data Units (BPDUs) bietet, kann dies in geswitchten Netzen durch Angreifer ausgenutzt werden. Wenn ein Angreifer von einer am Switch angeschlossenen Station in der Lage ist, BPDUs auszusenden, wird mit Hilfe des Spanning Tree-Algorithmus die Topologie neu berechnet. Die Konvergenz zur Berechnung der Topologie-Änderung kann beim Spanning-Tree 30 Sekunden betragen. Da für Loadbalancer in einer Hochverfügbarkeitsarchitektur Spanning Tree (mit Ausnahme der Hot-Standby-Konfiguration) praktisch immer zum Einsatz kommt, kann durch die Aussendung von BPDUs die Verfügbarkeit des Netzes empfindlich gestört werden.
G 5.115	**Überwindung der Grenzen zwischen VLANs** Virtual LANs (VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Ein VLAN bildet gleichzeitig eine separate Broadcast-Domäne. Das bedeutet, dass Broadcasts nur innerhalb des VLANs verteilt werden. Ein VLAN kann sich hierbei über ein ganzes geswitchtes Netz hinziehen und braucht nicht nur auf einen einzelnen Switch beschränkt zu bleiben. VLANs über mehrere Switches auszudehnen, wird durch unterschiedliche sogenannte Trunking-Protokolle realisiert. Hierbei wird pro Switch ein physischer Port für die Inter-Switch-Kommunikation reserviert, die logische Verbindung zwischen den Switches wird als Trunk bezeichnet. Ein Ethernet-Rahmen wird beim Informationsaustausch zwischen den Switches in das Trunking-Protokoll gekapselt. Dadurch ist der Ziel-Switch in der Lage, die Information dem entsprechenden VLAN zuzuordnen. Als Standards werden IEEE 802.1q und die proprietären Protokolle ISL(Inter Switch Link) und VTP (Vlan Trunking Protocol) verwendet. Wenn sich ein Angreifer, der an einem Switch angeschlossen ist beispielsweise durch die Verwendung der Trunking-Protokolle ISL oder IEEE 802.1q als Switch ausgibt, ist es möglich, dadurch auf alle konfigurierten VLANs Zugriff zu erhalten und so Daten mitzulesen, die zu einem VLAN gehören, auf das der Angreifer normalerweise keinen Zugriff hat. Da Loadbalancer in der Regel nur über eine begrenzte Anzahl von physischen Ports verfügen, ist das Trunking Protokoll IEEE 802.1q sehr häufig implementiert, wodurch die Geräte für diese Angriffe anfällig werden.
G 9.10	**Manipulation der Health-Ceck-Verfahren** Der Health-Check (Verfügbarkeitstest) ist ein grundlegender Bestandteil der Loadbalancer Software, über den sichergestellt werden soll, dass die Res-

	sourcen für die Lastverteilten Anwendungen auch tatsächlich noch verfügbar sind. Diese Verfügbarkeitstests reichen von einem Test der Links der angeschlossenen Geräte (IDS-Systeme) über simple Tests der Erreichbarkeit der Plattform (ICMP-Echo, TCP-Connect) und anwendungsspezifische Tests (z.B. http get zum Abfragen einer Webserver-Startseite) bis zur Ausführung komplexer Scripte, die die gleichzeitige Erfüllung mehrerer Kriterien erfordern, damit eine Ressource für die Lastverteilung als verfügbar gekennzeichnet wird. Gelingt es einem potentiellen Angreifer, ein solches Script derart zu manipulieren, dass eine Verfügbarkeitüberprüfung auch nur für ein Kriterium fehlschlägt, werden die betroffenen Ressourcen als nicht mehr verfügbar gekennzeichnet und für die Lastverteilung der entsprechende Anwendung nicht mehr berücksichtigt. Dies kann eine deutliche Leisungs-und /oder Verfügbarkeitseinbuße nach sich ziehen oder auch den totalen Ausfall der lastverteilten Anwendung.

2.3 Maßnahmenempfehlungen

Für die sichere Implementierung eines Loadbalancer ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Installation bis hin zum Betrieb. Nachfolgend wird das Maßnahmenbündel für den Baustein "Loadbalancer" vorgestellt:

2.3.1 Planung und Konzeption

M 2.278*	(Z)	**Typische Einsatzszenarien von Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Leiter IT, Administrator Der Einsatzzweck von Loadbalancer bestimmt maßgeblich die Konfiguration der Systeme. Zudem bestimmt die Verwendung auch die zusätzlichen Funktionen, die von einem Loadbalancer bereit gestellt werden müssen. Loadbalancer im internen Netz Loadbalancer können im internen Netz zum Einsatz gelangen, um Dienste und Anwendungen im Intranet hochverfügbar zu gestalten und gleichzeitig das Antwortverhalten zu verbessern. In dieser Funktion übernehmen sie häufig auch die Aufgabe eines LAN-to-LAN-Routers, da sich die Server nicht selten in einem separaten Subnetz befinden. Durch zu prinzipbedingte Anwendung von NAT (Network Address Translation) bei der Lastverteilung, kann der Anwender nicht mehr auf die Server selbst zugreifen, sondern nur noch auf das virtuelle Abbild desselben. Nur durch eine spezielle Konfiguration lässt sich dieser Mechanismus umgehen, so dass ein Angriff von innen auf die Server direkt erschwert ist. Bei diesem Einsatzszenario hängen die Sicherheitsanforderungen an den Loadbalancer stark vom Schutzbedarf der Teilnetze ab, die über den Loadbalancer verbunden sind. Loadbalancer in der DMZ Bei diesem Einsatzszenario bestehen dieselben funktionalen Zusammenhänge wie bei dem Einsatz im Intranet. Die Adressumsetzung NAT hat in diesem halböffentlichen Bereich jedoch neben dem praktischen Aspekt der Einsparung offizieller IP-Adressen auch den Sicherheitsaspekt, dass von außen nur auf die virtuelle Adresse mit genau dem vorgegebenen Dienst zugegriffen werden kann.

		Zu den Sicherheitsanforderungen an den Loadbalancer, die für den Einsatz im Intranet relevant sind, kommen hier der verstärkte Schutz der Management-IP-Adresse des Loadbalancers und der Schutz vor Denial-of-Service Angriffen hinzu. Loadbalancer zur Anbindung an externe Netze Wird ein Loadbalancer zur Anbindung des eigenen Netzes einer Organisation an externe Netze mehrerer ISP´s eingesetzt, so spricht man von einem WAN-Link-Loadbalancer mit der Funktion eines Border-Routers. Oft sind Border-Router auch in ein Sicherheits-Gateway integriert und übernehmen in diesem die Funktion des externen Paketfilters (siehe unten). Bei Loadbalancer, die an fremde Netze angeschlossen sind, spielt die Absicherung des Gerätes eine besonders wichtige Rolle, da sie Angriffen von außen direkt ausgesetzt sind. Loadbalancer als Paketfilter Loadbalancer werden oft als Bestandteil von Sicherheits-Gateways zum Anschluss an öffentliche Netze (beispielsweise das Internet) verwendet. Im folgenden Beispiel besteht der Sicherheits-Gateway aus einem internen Paketfilter, einem externen Paketfilter und einem Applikations-Gateway. Die festgelegten Filterregeln werden sowohl auf dem zentralen System als auch auf den Loadbalancer (intern und extern) konfiguriert. Auf den Loadbalancer wird das Regelwerk durch die Einrichtung von Access Control Lists (ACLs) etabliert.
M 2.279 *	(A)	**Erstellung einer Sicherheitsrichtlinie für Loadbalancer** Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: IT-Sicherheitsmanagement Da Loadbalancer zentrale Elemente eines Netzes sind, ist der sichere und ordnungsgemäße Betrieb besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist. Die zentralen sicherheitstechnischen Anforderungen (das zu erreichende Sicherheitsniveau) ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für Loadbalancer formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen. Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an

		der Beschaffung und dem Betrieb von Loadbalancern beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen. Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von Loadbalancern treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten: <u>Allgemeine Konfigurationsstrategie ("Liberal" oder "Restriktiv")</u> <u>Regelungen für die Arbeit der Administratoren und Revisoren</u> • Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)? • Welche Vorgänge werden müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt? • Gilt für bestimmte Änderungen ein Vieraugenprinzip? • Nach welchem Schema werden Administrationsrechte vergeben? <u>Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils</u> <u>Vorgaben für die Installation und Konfiguration</u> • Vorgehen bei der Erstinstallation • Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen • Regelungen zur physikalischen Zugriffskontrolle • Verwendung und Konfiguration von Konsole und sonstigen Zugriffsarten • Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden. • Regelungen zur Einrichtung und Nutzung von VLANs (beispielsweise: keine VLANs mit unterschiedlichem Schutzbedarf auf einem Switch) • Regelungen zu Erstellung und Pflege von Dokumentation, Form der Dokumentation: Verfahrensanweisungen, Betriebs-

		handbücher • Falls allgemeine Vorgaben existieren: Zugelassene und nicht zugelassene Dienste, Protokolle und Netze <u>Vorgaben für den sicheren Betrieb</u> • Absicherung der Administration (beispielsweise: Zugriff nur über abgesicherte Verbindungen) • Einsatz von Verschlüsselung (Standards, Schlüsselstärken, Einsatzbereiche) • Vorgaben zu Passwortnutzung (Passwortregeln, durch Passwörter zu schützende Bereiche, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern) • Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement • Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen <u>Protokollierung</u> • Welche Ereignisse werden protokolliert? • Wo werden die Protokolldateien gespeichert? • Wie und in welchen Abständen werden die Protokolle ausgewertet? <u>Datensicherung und Recovery (siehe auch M 6.91* Datensicherung und Recovery bei Loadbalancern)</u> • Einbindung in das organisationsweite Datensicherungskonzept <u>Störungs- und Fehlerbehandlung, Incident Handling</u> • Regelungen für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung) • Regelungen für Sicherheitsvorfälle <u>Notfallvorsorge (siehe auch M 6.92* Notfallvorsorge bei Loadbalancern)</u> • Einbindung in das organisationsweite Notfallvorsorgekonzept <u>Revision und Audit (Verantwortlichkeiten, Vorgehen, Integration in ein übergreifendes Revisionskonzept)</u> Die Verantwortung für die Sicherheitsrichtlinie liegt beim IT-

		Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen. Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.
M 2.314*	(Z)	**Verwendung von hochverfügbaren Architekturen** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator Die Verfügbarkeit von Anwendungen und Diensten hängt von der Funktion des Loadbalancers ab. Je mehr Anwendungen aber über einem Loadbalancer laufen, desto ausfallsicherer muss dieser sein. Ein Loadbalancer enthält in der Regel verschiedene potentielle Fehlerquellen ("Single Points of Failure"), also Komponenten, deren Ausfall den Ausfall des Gesamtsystems auslösen kann: CPU, Festplatten, Stromversorgung, Lüfter, Backplane, etc. Die Wiederherstellung des Gesamtsystems kann in diesem Fall erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen können zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden: <u>Cold-Standby</u> Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht aktiv ist. Wenn das erste System ausfällt, kann das Ersatzssystem manuell hochgefahren und ins Netz integriert werden. Nach der Vorhaltung von einzelnen Ersatzteilen ist dies die einfachste Redundanz-Lösung. <u>Hot-Standby</u> Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem bereit, das aber neben dem Produktivsystem parallel in Betrieb gehalten wird. Die Funktion des Produktivsystems wird überwacht, bei Ausfall wird das Ersatzsystem aktiv. Der Wechsel kann automatisch erfolgen oder

		auch manuell. Für den automatischen Wechsel sind zusätzliche Funktionalitäten im Gesamtsystem erforderlich z. B. die automatische Erkennung von Ausfällen über eine dedizierte Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand des Ersatzsystems kontinuierlich überprüft werden. Verwendung von Layer-3 Redundanzprotokollen Da Loadbalancer in typischen Einsatzszenarien Routingfunktionen übernehmen und somit Gateway für die konfigurierten Subnetze darstellen, kann beim Einsatz von 2 Loadbalancern unter Verwendung der Protokolls VRRP (Virtual Router Redundanc Protokoll) ein Single Point of Failure vermieden werden. Je nach Implementierung dieses Protokolls können Active-Standby oder Active-Active Konfigurationen realisiert werden. Dabei erfolgt die Auswahl des VRRP-Masters anhand der aktuellen Priorität für ein bestimmtes Interface. Weitergehende herstellerspezifische Implementierungen erlauben u.a. die dynamische Veränderung der Prioritäten anhand der Anzahl der aktiven Interfaces, aktiven Ports oder weiterer L4 Parameter. Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden.

2.3.2 Beschaffung

M 2.280*	(C)	**Kriterien für die Beschaffung und geeignete Auswahl von Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Aktive Netzkomponenten unterscheiden sich in ihrem Leistungsumfang, den angebotenen Sicherheitsmechanismen, Bedienkomfort und Wirtschaftlichkeit. Werden bei der Beschaffung Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneten Geräten das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist. Bevor Loadbalancer beschafft werden, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine

		fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt. Aus dem Blickwinkel der IT-Sicherheit sind zentrale Anforderungen an aktive Netzkomponenten, dass diese die Administration über sichere Protokolle erlauben und dass die Benutzerverwaltung des Geräts es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen. Die Anforderung, dass Passwörter nur verschlüsselt im Gerät gespeichert werden dürfen, sollte eigentlich eine Selbstverständlichkeit sein, jedoch gibt es immer noch Geräte, bei denen Passwörter im Klartext in Konfigurationsdateien gespeichert werden müssen. Bei Neubeschaffungen sollten keine Geräte mehr berücksichtigt werden, die keine sichere Administrationsmöglichkeit bieten und bei denen es nicht möglich ist, Passwörter verschlüsselt abzuspeichern. Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Loadbalancern aufgelistet. Allgemeine Kriterien für Loadbalancer: • Grundlegende funktionale Anforderungen (Serverloadbalancing Layer 4-7, Network Address Translation NAT, Routing etc.) • Sicherheit • Wartbarkeit • Zuverlässigkeit/Ausfallsicherheit • Benutzerfreundlichkeit • Kosten • Funktionalität • Protokollierung • Infrastruktur

2.3.3 Umsetzung

M 1.43	(A)	**Gesicherte Aufstellung aktiver Netzkomponenten** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Planer Verantwortlich für Umsetzung: Leiter Haustechnik, Administrator Um den manipulationssicheren Betrieb eines Netzes sicherzustellen, ist es erforderlich, aktive Netzkomponenten wie z.B. Loadbalancer, in einer gesicherten Umgebung zu betreiben. Dies kann entweder ein Serverraum sein (siehe Baustein B 2.4 Serverraum) oder, wenn kein separater Serverraum zur Verfügung steht, ein Serverschrank (siehe Baustein 4.4 Schutzschränke). Unbefugte Personen dürfen zum Aufstellungsort der Geräte keinen unbeaufsichtigten Zugang erhalten. Dabei sollte beachtet werden, dass Hersteller von Schutzschränken oft Standardschlösser einsetzen, so dass mit einem beliebigen Schlüssel des Schrankherstellers alle Schränke geöffnet werden können. Daher muss gegebenenfalls das serienmäßige Schloss eines Schutzschranks gegen ein individuelles Schloss ausgetauscht werden. Außerdem sollten die Geräte so aufgestellt werden, dass sie vor elektromagnetischen oder magnetischen Feldern geschützt sind. Zusätzlich sollten sie mit Kontrollmechanismen ausgestattet sein, die eine Überschreitung der zulässigen Toleranzen bei Feuchtigkeit und Temperatur signalisieren. Der Schutz von Loadbalancer vor unbefugtem Zugriff ist auch deswegen sehr wichtig, weil für viele Geräte Passwort-Recovery-Prozeduren für das Rücksetzen von Passwörtern bekannt sind, die zumeist den physikalischen Zugang zu den Geräten (Konsolenanschluss) voraussetzen. Das serielle Konsolen-Interface (RS-232-Port) ermöglicht den Anschluss eines PC oder Terminals, um Administrations- oder Konfigurationsarbeiten durchzuführen. Das Passwort für den Zugriff auf die Konsole muss schriftlich an einem sicheren Ort hinterlegt sein (siehe dazu auch unter M 2.22 Hinterlegen des Passwortes im GSHB). Zusätzlich muss den Gefahren durch Diebstahl, Vandalismus und unbefugtem Ausschalten des Geräts vorgebeugt werden.

M 3.38*	(A)	**Administratorenschulung für Loadbalancer (Loadbalancer)** Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement Für den sicheren Betrieb von Loadbalancer ist es wichtig, dass alle Arbeiten durch Personal durchgeführt werden, das in der Lage ist, alle gebotenen Funktionen und Sicherheitsmerkmale optimal zu nutzen. Daher ist es unerlässlich, dass die Administratoren entsprechend geschult werden. In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb von Loadbalancern notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte zum gewählten Produkt. In dieser Maßnahme werden Anforderungen an Schulungen beschrieben, die Administratoren in die Lage versetzen, Loadbalancer in einer typischen Umgebung installieren und betreiben zu können. In den Schulungen sollten die Grundlagen, Konzepte und Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche vermittelt werden. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen. <u>Grundlagen</u> • ISO/OSI Schichten Modell • Netztopographien / -topologien und Übertragungstechniken • Verkabelung • Aktive Netzkomponenten • Grundlagen von IP und der damit zusammenhängenden Protokolle (IP-Adressierung, Subnetting, IP, ICMP, TCP, UDP) • Überblick über Hersteller und Produkte <u>Switching</u> • Funktionsweise eines Switches • Transparent Bridging Funktion (IEEE 802.1d) • Spanning Tree Algorithmus (IEEE 802.1d) • VLAN (VLAN Typen, Tagging, IEEE 802.1q)

		Routing • Funktionsweise eines Routers • Statisches und dynamisches Routing • Dynamische Routing-Protokolle (RIPv1, RIPv2, OSPFv2, BGPv4) Loadbalancing (Lastverteilung) • Funktionsweise des Basis-Serverloadbalancings • Health-Checks für Anwendungsresourcen (Server) • Kriterien für das Loadbalancing (Round Robin, Antwortzeiten, Bandbreite, Verbindungsanzahl etc.) • Steuerungsmöglichkeiten (Gewichtung, max. Verbindungsanzahl der Server) • Backup-/Überlaufserver • Inhalte basierendes Loadbalancing • Umleiten von Diensteanforderungen • Filtern und NAT Einrichtung • Einrichtung und Konfiguration von Loadbalancer Betrieb • Management der Geräte, Werkzeuge • Integration in Netzmanagementsysteme (NMS) • Protokollierung (syslog) • Sicherung und Verwaltung von Konfigurationsdateien Fehlerbehebung • Fehlerquellen und Ursachen • Mess- und Analysewerkzeuge • Teststrategien zur Fehlersuche • Anforderungen an sichere Netzinstallationen IT-Sicherheit • Grundlagen der IT-Sicherheit sowie für Loadbalancer relevante IT-Sicherheitsaspekte • Authentisierung, Autorisierung

		• Kryptoverfahren und Anwendungen • Angriffsszenarien (Denial of Service Attacken, ARP-Spoofing, IP-Spoofing) und geeignete Schutzmaßnahmen • Gefahrenquelle "Default-Einstellungen" • Vorsorgemaßnahmen, Reaktion und Analyse • Incident Handling
M 4.201*	(A)	**Sichere lokale Grundkonfiguration von Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Sämtliche Konfigurationsarbeiten an Loadbalancer müssen entsprechend der erstellten Sicherheitsrichtlinie (siehe M 2.279* Erstellung einer Sicherheitsrichtlinie für Loadbalancer) durchgeführt werden und wie in M 2.281* Dokumentation der Systemkonfiguration von Loadbalancer beschrieben dokumentiert und kommentiert werden. Betriebssystem Da Loadbalancer durch ihren Einsatz im Netz eine besonders große Anzahl von Kommunikationspartnern und damit potentiellen Angreifern haben, ist bei der Auswahl und Pflege des Betriebssystems besondere Sorgfalt notwendig. Zunächst ist es wichtig, sich einen Überblick über die benötigten und angebotenen Funktionen zu verschaffen. Das Ziel bei der Auswahl sollte sein, eine möglichst stabile Version zu betreiben. Hierbei ist zu beachten, dass mit dem Alter eines Release in der Regel auch die Zahl der Angriffsmöglichkeiten (Exploits) zunimmt. Andererseits kann ein sehr neues Release (insbesondere mit völlig neuen Funktionen) noch Unzulänglichkeiten oder neue Fehler enthalten. Im Zweifelsfall ist es meist besser, eine ältere Version einzusetzen, falls diese den funktionalen Anforderungen noch genügt. Allerdings müssen für diese unbedingt die aktuellen Sicherheitspatches eingespielt werden (siehe auch M 2.273* Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates). Versionen, für die vom Hersteller keine Sicherheitspatches mehr zur Verfügung gestellt werden, sollten nicht mehr eingesetzt werden. Offline-Grundkonfiguration Bevor ein Loadbalancer an das Produktions-Netz angeschlossen wird, muss eine sichere Grundkonfiguration hergestellt werden. Häufig werden Geräte vom Hersteller mit einer Default-Konfiguration aus-

		geliefert, die vor allem auf eine schnelle Inbetriebnahme mit möglichst umfassender Funktionalität ausgerichtet ist und in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher müssen die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline oder nur in einem eigens dafür eingerichteten und besonders gesicherten Testnetz erfolgen. Oft ist es möglich, die Konfiguration mit entsprechenden Programmen auf einem Management-Rechner zu erstellen und beispielsweise mit einer Speicherkarte auf das neue Gerät zu übertragen. Ist nur eine Übertragung über das Netz möglich, so darf dies nur im Testnetz oder im Administrationsnetz geschehen. Bei der Konfiguration muss beachtet werden, dass unter Umständen nicht jedes Administrations- oder Konfigurationswerkzeug (Konsole, Webschnittstelle, externes Konfigurationsprogramm) alle relevanten Informationen anzeigt. So kann es beispielsweise vorkommen, dass die Systembefehle zur Anzeige einer Konfiguration auf Loadbalancern nicht alle Parameter anzeigen. Daher ist es wichtig, anhand der vorhandenen Dokumentation nachzuvollziehen, dass auch alle relevanten Einstellungen vorgenommen wurden. Es bietet sich an, die Grundkonfiguration in zwei Schritte zu unterteilen: • Lokale Konfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf das Gerät selbst beziehen (beispielsweise Benutzerkonten oder -rollen, Passwörter, Protokolldateien, Einstellungen für Konsolenzugang und serielle Schnittstelle, etc.). Die entsprechenden Schritte sind im Anschluss beschrieben. • Netzkonfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf die Funktion des Gerätes im Netz beziehen (beispielsweise Dienste und Protokolle, Einrichtung von Access-Control-Listen (ACLs), VLANs etc.). Die entsprechenden Schritte sind in M 4.202* Sichere Netz-Grundkonfiguration von Loadbalancern beschrieben. <u>Benutzerkonten und Passworte</u> Die Möglichkeiten für die Einrichtung von Benutzern und Rollen und das Zuweisen von Berechtigungen unterscheiden sich von Hersteller zu Hersteller (gelegentlich auch zwischen einzelnen Geräten oder Software-Releases) teilweise erheblich. Daher ist es empfehlenswert, entsprechend dem vorgegebenen Rechte- und Rollenkonzept für die Administration der aktiven Netzkomponenten ein detailliertes Konzept für die jeweiligen Geräte zu erstellen.

		Auf Loadbalancern einiger Hersteller sind werksmäßig mehrere Benutzerkonten (Accounts) mit abgestuften Berechtigungen für die Administration vorhanden. Andere Geräte sind werksmäßig nur mit einem Benutzerkonto für Administrationszwecke voreingestellt. Voreingestellte Benutzerkonten haben allgemein bekannte Standardnamen und Passwörter, gelegentlich sind Administrations-Accounts sogar ganz ohne Passwort vorkonfiguriert. Auf einschlägigen Internet-Seiten können Listen mit herstellerspezifischen Standard-Accounts und Passwörtern heruntergeladen werden. Bei der Inbetriebnahme des Geräts müssen diese Standard-Benutzerkonten, falls möglich, geändert werden. In jedem Fall müssen aber die Passwörter der Standard-Accounts geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden. Entsprechend dem Rechte- und Rollenkonzept müssen anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden. Leider werden bei vielen aktiven Netzkomponenten Passwörter im Klartext in den Konfigurationsdateien gespeichert. Insbesondere falls dies der Fall ist, müssen Konfigurationsdateien vor unbefugtem Zugriff besonders geschützt werden. Wo immer es möglich ist, eine verschlüsselte Speicherung von Passwörtern zu konfigurieren, sollte von dieser Möglichkeit Gebrauch gemacht werden. Weitergehende Aspekte sind in M 1.43 Gesicherte Aufstellung aktiver Netzkomponenten, M 4.204* Sichere Administration von Loadbalancern und M 6.91* Datensicherung und Recovery bei Loadbalancern beschrieben. <u>Login-Banner</u> Beim Login wird auf den Geräten meist eine relativ ausführliche Login-Nachricht angezeigt. In dieser Login-Nachricht sind oft Informationen (beispielsweise Modell- oder Versionsnummer, Software-Release-Stand oder Patchlevel) enthalten, die einem potentiellen Angreifer von Nutzen sein können. Sofern das Gerät es zulässt, sollte die Standard-Loginnachricht durch eine angepasste Version ersetzt werden, die diese Informationen nicht mehr enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems darf unter keinen Umständen vom Login-Banner verraten werden. Stattdessen sollten folgende Informationen bei einer Anmeldung am Gerät angezeigt werden: • Jeglicher Zugriff darf nur durch autorisiertes Personal erfolgen. • Alle Arbeiten sind entsprechend der Sicherheitsrichtlinie durchzuführen. • Das Gerät ist in zentrale Kontrollmechanismen, wie beispielsweise in ein Netzmanagementsystem (NMS) zur Protokollie-

		rung und Erkennung von Verstößen gegen die Sicherheitsrichtlinie eingebunden. • Verstöße gegen die Sicherheitsrichtlinie werden disziplinarisch / strafrechtlich verfolgt. <u>Protokollierung</u> Sicherheitsmaßnahmen in Bezug auf die Protokollierung auf Netzkomponenten und der Einbindung von Zeitinformationen mit Hilfe von NTP sind in M 4.205* Protokollierung bei Loadbalancern beschrieben. <u>Schnittstellen</u> Auf Loadbalancern sollten alle nicht genutzten Ports entweder deaktiviert oder einem eigens dafür eingerichteten "Unassigned-VLAN" zugeordnet werden. <u>Backup der Konfiguration</u> Die Konfigurationsdateien der Grundkonfiguration bilden die Basis für die weitere Konfiguration. Es wird empfohlen, sowohl von den mit dem Gerät ausgelieferten Default-Konfigurationsdateien als auch von den Dateien, die das Ergebnis der Grundkonfiguration darstellen, Sicherungskopien zu erstellen.
M 4.202*	(A)	**Sichere Netz-Grundkonfiguration von Loadbalancer** Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT Verantwortlich für Umsetzung: Administrator <u>Remote-Zugriff</u> Für die Administration aktiver Netzkomponenten über das Netz wird oft noch Telnet als Standardmöglichkeit angeboten. Oft gibt es auch eine Administrationsmöglichkeit über SNMP oder den Zugriff über eine HTTP-Schnittstelle. Alle diese Protokolle haben den Nachteil, dass sowohl Benutzername und Passwort als auch die Nutzdaten im Klartext über das Netz übertragen werden (siehe auch G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen). Daher ist für die Administration entweder ein eigenes Administrationsnetz (Out-of-Band-Management) einzurichten, oder es dürfen nur Protokolle benutzt werden (beispielsweise ssh2), die eine gesicherte Authentisierung und verschlüsselte Übertragung unterstützen. Soll SNMP außerhalb eines eigenen Administrationsnetzes eingesetzt werden, so darf nur SNMPv3 benutzt werden. <u>Authentisierungsserver</u>

		In großen Netzen sollten Loadbalancer möglichst für die Nutzung von Authentisierungsservern unter Verwendung von Einmal-Passwörtern konfiguriert werden. Beispiele hierfür sind RADIUS oder TACACS+. Weitergehende Aspekte sind in M 4.204* Sichere Administration von Loadbalancer beschrieben. Management-Interface und Administrationsnetz Einige Geräte bieten die Möglichkeit, ein eigenes logisches Interface zur Administration (Management-Interface) zu konfigurieren. Bei Loadbalancern sollte dieses Interface einem eigenen VLAN zugeordnet werden, das ausschließlich für administrative Zwecke verwendet wird (Out-of-Band Management) und dem ausschließlich Management-Interfaces angehören. Außerdem sollten ACLs so konfiguriert werden, dass der Zugriff auf das Management-Interface von der Management-Station aus mit definierten Protokollen erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren. Weitere Schritte zur Einrichtung eines Administrationsnetzes (Out-of-Band-Management) sind in M 4.204* Sichere Administration von Loadbalancern beschrieben. Deaktivierung unnötiger Netzdienste Hersteller aktiver Netzkomponenten legen oft in erster Linie Wert auf eine möglichst einfache Inbetriebnahme und Konfiguration der Komponenten. Daher ist in der Default-Konfiguration meist eine Vielzahl von Diensten aktiviert. Es sollten nur Dienste aktiviert sein, die für den Betrieb notwendig sind. Nicht benötigte Dienste auf den Loadbalancern müssen deaktiviert werden, weil sie ein erhöhtes Risiko darstellen. Generell dürfen diese Dienste nicht aus unsicheren Netzen erreichbar sein. Dies ist durch entsprechende Access-Control-Lists sicherzustellen. Anti-Spoofing Border-Router stellen den Übergang von internen Netzen zu externen Netzen dar. Auf Border-Routern sollten Sicherheitsmaßnahmen ergriffen werden, die IP-Spoofing (siehe auch G 5.48) verhindern. Dies kann beispielsweise durch die Einrichtung entsprechender ACLs erreicht werden. Eine mögliche Variante ist folgender Ansatz: • An den externen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse im internen Netz liegt. • An den internen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse nicht im internen Netz liegt. Zumindest bei Paketen, die auf Grund der zweiten Regel blockiert werden, sind eine entsprechende Protokollierung und gegebenenfalls eine Alarmierung der zuständigen Administratoren empfehlenswert.

		Die Tatsache, dass eine Station innerhalb des eigenen Netzes offensichtlich gefälschte Pakete verschickt, ist nämlich ein klares Indiz dafür, dass entweder eine falsche Konfiguration oder gar ein Sicherheitsproblem vorliegt. Routing-Protokolle Es sollten nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung unterstützen. In demilitarisierten Zonen dürfen keine dynamischen Routing-Protokolle eingesetzt werden, stattdessen müssen statische Routen eingetragen werden. Die Verwendung von Routing-Protokollen sollte zusätzlich durch die Einrichtung von ACLs abgesichert sein. Mehr Informationen finden sich in M 5.112 Sicherheitsaspekte von Routing-Protokollen. Access Control Lists Die Verwendung von Access Control Lists (ACLs) zur Einschränkung des Zugriffes auf Loadbalancer und zur netzübergreifenden Paketfilterung ist in M 5.112 Sicherheitsaspekte von Routing-Protokollen beschrieben. Ein weiterer Grund für die Verwendung von Access Control Lists ist die Tatsache, dass über den Loadbalancer eine Kommunikation aller angeschlossenen Server untereinander möglich wäre. Im Fall der Kompromittierung eines dieser Server, hätte ein potentieller Angreifer eine gute Chance auch auf die anderen Server und Systeme zuzugreifen. Durch die Anwendung der ACLs kann diese Kommunikation auf bestimmte Dienste beschränkt oder generell unterbunden werden. Spanning Tree Das Spanning Tree Protocol (STP, IEEE 802.1d) wird von Switches und Bridges verwendet, um Schleifenbildungen innerhalb des Netzes auf der OSI-Schicht 2 zu vermeiden. Es werden BPDUs (Bridge Protocol Data Units) ausgesendet, um die Root-Bridge (basierend auf MAC-Adresse und Priorität) zum Systemstart und bei Topographie-Änderungen zu bestimmen. Dieses Protokoll bietet keine Authentisierung. Deshalb sollte STP zumindest auf allen Endgeräte-Ports deaktiviert werden. In der Konfiguration muss eine eindeutige Root-Bridge festgelegt werden. VLANs und Trunking Trunking ermöglicht es, VLANs über mehrere Switches auszudehnen. Die Steuerung von Trunking wird durch den Standard IEEE 802.1q oder durch unterschiedliche proprietäre Trunking-Protokolle realisiert. Dabei wird pro Switch ein physischer Port (Trunk-Port) für die Inter-Switch-Kommunikation reserviert. Diese logische Verbindung zwi-

		schen den Switches wird als Trunk bezeichnet. Trunk-Ports können auf alle VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs dieses Trunks ermöglicht. Manche Geräte bieten allerdings auch die Möglichkeit, den Zugriff eines Trunk-Ports auf bestimmte VLANs zu beschränken ("VLAN Pruning"). Sofern ein Switch eine solche Möglichkeit bietet, ist es empfehlenswert, dies zu nutzen. Auf Endgeräte-Ports sollte Trunking möglichst deaktiviert werden. Das Default-VLAN darf nicht für ein produktives VLAN verwendet werden. Freie Ports Nach Möglichkeit sollten nicht genutzte Ports allerdings ganz deaktiviert werden, da die VLAN-Port-Zuweisung in ein Unassigned-VLAN nur wenig zusätzliche Sicherheit bietet.
M 4.203 *	(A)	**Konfigurations-Checkliste für Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Zusammenfassend können anhand der folgenden Konfigurations-Checkliste die wichtigsten sicherheitsrelevanten Einstellungen auf Loadbalancern geprüft werden. Es muss jedoch festgehalten werden, dass die sichere Konfiguration von Loadbalancern stark vom Einsatzzweck abhängt. Beispielsweise muss auf Loadbalancern mit Border-Router-Funktion die Einrichtung von ACLs, Anti-Spoofing-Konfiguration, etc. berücksichtigt werden. Deshalb sollte die folgende Tabelle lediglich als allgemeine Anleitung verwendet werden. Konfigurations-Checkliste für Loadbalancer • Erstellung einer Sicherheitsrichtlinie für Loadbalancer • Prüfung und gegebenenfalls Update des Betriebssystems • Die Loadbalancerkonfiguration offline speichern, sichern und gegen unbefugten Zugang schützen (Nutzung eines TFTP-Servers nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz)) • Dokumentation und Kommentierung der Konfiguration • Konfiguration von Passwortschutz für alle Zugänge (Konsole, VTY, etc.) • Einrichtung eines Session-Timeouts

		• Keine Trivial-Passworte verwenden • Verschlüsselte Speicherung der Passworte • Einrichtung eines physischen Zugangsschutzes für den Konsolenanschluss • Für Administrationszwecke soweit möglich TELNET durch SSH ersetzen • Möglichst RADIUS oder TACACS+ zur Authentisierung verwenden • Einschränkung der Administrationszugänge (z. B. SSH, SNMP, TELNET) durch ACLs, Nutzung von SNMP und TELNET nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz), bei SNMP Änderung der Community-Strings • Deaktivieren unnötiger Netzdienste • nicht benötigte Ports in "Unassigned VLAN" verschieben oder ebenfalls deaktivieren • Kritische Schnittstellendienste und Protokolle sperren • Protokollierung einschalten • Genaue Uhrzeit auf den Geräten einstellen (interner NTP-Server) • Einbinden der Zeitinformation bei der Protokollierung • Auswerten, Überprüfen und Archivieren der Protokolldateien entsprechend der Sicherheitsrichtlinie • SNMP möglichst deaktivieren, Nutzung nur in Verbindung mit Out-of-Band-Management (Administrationsnetz) oder Verwendung von SNMPv3 • Überprüfung der Default-Einstellungen • Einrichtung eines geeigneten Login-Banners • Deaktivierung von Trunk-Negotiation auf Endgeräte-Ports • Das Default-VLAN darf nicht genutzt werden • Einrichtung eines eigenen VLANs für alle Trunk-Ports • Einrichtung eines Unassigned-VLANs für alle unbenutzten Ports • Deaktivierung von STP (Spanning Tree) auf Engeräte-Ports • Festlegung einer Root-Bridge

		• Erstellung einer Kommunikationsmatrix des netzübergreifenden Datenverkehrs • Begrenzen des netzübergreifenden Datenverkehrs in Abgleich mit Kommunikationsmatrix durch Zugriffslisten • Blockieren von unbekannten Adressen durch Zugriffslisten (ACLs) • Konfiguration statischer Routen im DMZ-Bereich • Konfiguration von Integritätsmechanismen der verwendeten Routing Protokolle
M 5.111*	(C)	**Einrichtung von Access Control Lists auf Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Die vielfältigen Zugriffsmöglichkeiten für die Nutzung und die Administration von Loadbalancer können mit Hilfe von Access Control Lists (ACLs) kontrolliert werden. Der Zugriff kann für einzelne Rechner oder Netze und für die jeweilige Zugriffsmethode festgelegt werden. Mittels der ACL erfolgt die Festlegung, welche Rechner oder Netze auf den Loadbalancer über Dienste wie bspw. TELNET, SNMP, HTTP, etc. zugreifen können. Die Festlegung der ACLs muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Insbesondere sollte ein generelles Vorgehen für den Fall festgelegt werden, dass keine spezifischen Regeln existieren. In diesem Zusammenhang gibt es grundsätzlich die beiden Ansätze "Was nicht verboten ist, ist erlaubt" (Blacklist) und "Was nicht erlaubt ist, ist verboten" (Whitelist). Bei der Konfiguration sollte generell der restriktivere Whitelist-Ansatz bevorzugt werden, da beim reinen Blacklist-Ansatz nahezu zwangsläufig Lücken bestehen bleiben. Mit Hilfe von ACLs kann nicht nur der Zugriff auf den Loadbalancer selbst, sondern auch der Datenverkehr über den Loadbalancer kontrolliert werden, da sie den Zugriff der angeschlossenen Endsysteme untereinander einschränken. Loadbalancer können auch als sehr komplexe, schnelle Paketfilter (je nach Modell in Wirespeed) in lokalen Netzen eingesetzt. Der Loadbalancer kontrolliert in diesem Fall den Datenverkehr pro Interface und Richtung (inbound und outbound) zwischen den angeschlossenen Endgeräten und Subnetzen.

		In der Regel werden innerhalb einer ACL mindestens folgende Kriterien ausgewertet: • Quelladresse (IP-Adresse im IP-Header) des Pakets • Zieladresse (IP-Adresse im IP-Header) des Pakets • Verwendetes Protokoll und gegebenenfalls Portnummer (z. B. Port 80/TCP für HTTP oder 25/TCP für SMTP) Zum Erkennen von Problemen wie beispielsweise Konfigurationsfehlern oder Angriffsversuchen im Netz sind ACLs immer derart zu konfigurieren, dass abgewiesene Zugriffsversuche protokolliert werden. Hierzu ist jedem Eintrag in der ACL das entsprechende Protokoll-Kommando anzufügen. Die Protokolldateien werden so zu einer wertvollen Datenquelle im Umgang mit Problemen und Angriffen im Netz. Die Erstellung einer ACL muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Nach Möglichkeit sollten Vorlagen (Templates) erstellt werden, die immer wieder verwendet werden können und nur gegebenenfalls geringfügig modifiziert werden müssen.

2.3.4 Betrieb

M 2.35	(B)	**Informationsbeschaffung über Sicherheitslücken des Systems** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen werden. Sicherheitsrelevante Updates oder Patches für die eingesetzte Hard- und Software müssen gegebenenfalls installiert werden (siehe auch M 2.273* Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates). Sind keine entsprechenden Updates oder Patches verfügbar, so muss eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden. Es ist daher sehr wichtig, dass sich die Systemadministratoren regelmäßig über neu bekannt gewordene Schwachstellen informieren.

		Idealerweise sollten sich die Administratoren und der IT-Sicherheitsbeauftragte bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine "unabhängige" Informationsquelle zu benutzen. Die Administratoren sollten jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, muss rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann.
M 2.273	(A)	**Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator Häufig werden Fehler in Software-Produkten bekannt, die dazu führen können, dass die Sicherheit der IT-Systeme, auf denen diese Produkte installiert sind, beeinträchtigt wird. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben. Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren (siehe auch M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems). Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten

		Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde. Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Vor der Installation eines Updates oder Patches sollte stets eine Datensicherung des Systems erstellt werden, das es ermöglicht, den Originalzustand wieder herzustellen, falls Probleme auftreten. Dies gilt insbesondere dann, wenn ausführliche Tests aus Zeitgründen oder mangels eines geeigneten Testsystems nicht durchgeführt werden können. In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden (siehe auch M 2.34 Dokumentation der Veränderungen an einem bestehenden System). Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System dadurch gefährdet ist.
M 2.281*	(A)	**Dokumentation der Systemkonfiguration von Loadbalancer** Verantwortlich für Initiierung: IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Die Konfiguration von Loadbalancer (Loadbalancer) wird meist mittels Konfigurationsdateien vorgenommen, die auf dem Gerät gespeichert sind. Loadbalancer besitzen eine Reihe von Konfigurationsoptionen, die für den sicheren Betrieb wichtig sind. Bei der Erstinstallation beziehungsweise im Auslieferungszustand sind diese Einstellungen mit Default-Werten belegt. Die Konfiguration, die bei der Inbetriebnahme des Geräts vorgenommen wird, muss so dokumentiert werden, dass sie jederzeit vom Administrator oder seinem Vertreter nachvollzogen werden kann. Insbesondere dann, wenn eine Konfiguration von einem Default-Wert abweicht, sollte in einem Kommentar in der Konfigurationsdatei festgehalten werden, warum die Einstellung so gewählt wurde. Jede Änderung der Konfiguration sollte vom Administrator

		nachvollzogen werden können. Es wird empfohlen, mindestens folgende Punkte zu dokumentieren: • Welche Änderung wurde durchgeführt? • Warum wurde die Änderung durchgeführt (Anlass)? • Wann wurde diese Änderung durchgeführt (Uhrzeit, Datum)? • Wer hat die Änderung durchgeführt? Die Dokumentation der Änderungen kann ebenfalls durch Kommentare in der Konfigurationsdatei erfolgen. Dabei ist es jedoch in der Regel sinnvoll, zu jeder Option nur die jeweils letzte Änderung in der Datei selbst zu speichern. Zusätzlich dazu sollten zumindest alle sicherheitsrelevanten Konfigurationsänderungen in einem Protokoll gespeichert werden, anhand dessen sich jederzeit nachvollziehen lässt, wie das Gerät zu einem bestimmten Zeitpunkt konfiguriert war. Dieses Protokoll sollte nicht auf dem Gerät selbst gespeichert werden. Die Konfigurationsdateien sollten zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert werden. Für die zentrale Verwaltung von Konfigurationsdateien werden oft TFTP-Server verwendet. TFTP-Server sollten jedoch nur in einem abgesicherten Administrationsnetz betrieben werden, weil der Dienst TFTP eine Reihe von Schwachstellen beinhaltet (siehe auch G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen). Eine Alternative dazu ist die Übertragung per SCP (siehe auch M 5.64 Secure Shell).
M 2.282 *	(A)	**Regelmäßige Kontrolle von Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Zur Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten und der Korrektheit aller Konfigurationsparameter ist ein regelmäßiger, möglichst automatisierter, Kontrollprozess zu etablieren. Hierzu gehören beispielsweiseregelmäßige Funktionstests, Veranlassen von Änderungen und Prüfung der Umsetzung sowie die Überprüfung der Logfiles und Alarme. Um die im laufenden Betrieb entstehende große Menge an relevanten Daten effektiv verarbeiten zu können, ist meist der Einsatz geeigneter Werkzeuge für eine möglichst weit automatisierte Kontrolle erforderlich. Dies kann beispielsweise durch die Einbindung in ein Netzmanagementsystem (NMS) geschehen.

		Checkliste für die Kontrolle Für die Kontrolle kann die Checkliste in M 4.203 Konfigurations-Checkliste für Router und Switches verwendet werden. Als Basis sollte die erstellte Sicherheitsrichtlinie für Router und Switches dienen (siehe M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches). Zusätzlich sollten folgende Punkte im Rahmen des Kontrollprozesses berücksichtigt werden: Was wird getestet bzw. kontrolliert? • Die generelle Funktionsfähigkeit von Geräten wird im Normalfall regelmäßig durch den Administrator im laufenden Betrieb geprüft. • Die Integrität von Konfigurationsdateien sollte in regelmäßigen Abständen geprüft werden. Die Sicherheitsrichtlinie für Router und Switches sollte eine regelmäßige Überprüfung mit Festlegung von Verantwortlichkeiten vorschreiben. • Der Stand der Datensicherung (zentral gespeicherte Konfigurationsdateien) sollte regelmäßig vom Administrator geprüft werden. • Die Systemdokumentation sollte laufend vom Administrator aktualisiert werden. Die Aktualität kann im Rahmen von Audits geprüft werden. • Hierzu sind auch M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile und M 2.64 Kontrolle der Protokolldateien zu berücksichtigen. Wie wird getestet? • Durch die Einbindung der Komponenten in ein Netzmanagement-System kann eine regelmäßige Kontrolle sichergestellt werden. Sicherheitsverletzungen, Ausfälle und Fehlfunktionen können mit Hilfe von Alarmierungsfunktionen des NMS zeitnah erkannt werden. • Im Rahmen von Audits erfolgt meist eine stichprobenartige Kontrolle von Komponenten. Als Basis für ein Audit dient die erstellte Sicherheitsrichtlinie für Loadbalancer. Wichtiger Bestandteil einer solchen Untersuchung ist die Aktualität der Systemdokumentation, Stand der Datensicherung, Passwortwechsel, etc. Unter Zuhilfenahme der Checkliste aus M 4.203* Konfigurations-Checkliste für Loadbalancer kann ein Großteil der sicherheitsrelevanten Einstellungen abgefragt werden. • Es existiert eine Reihe frei verfügbarer Sicherheits-Tools (z. B.

		Nessus), welche die Sicherheitseinstellungen auf Loadbalancern prüfen können. Solche Tools können auf einem Rechner im Netz installiert sein. Es sollte nach Möglichkeit die aktuellste Version verwendet werden. Als Betriebssystem ist oft Unix bzw. Linux notwendig. Von diesem System aus kann der Administrator die Loadbalancer scannen, um somit eine Vielzahl von Einstellungen dieser Geräte zu prüfen. Kommerzielle Tools bieten teilweise recht komfortable Auswertungen und Möglichkeiten zur Historienverfolgung der durchgeführten Scans. • Eine Vielzahl von Sicherheitsunternehmen bieten regelmäßige Überprüfungen von IT-Systemen an, im Rahmen derer auch die Loadbalancer getestet werden sollten. Durch turnusmäßige Berichte und Auswertungen erhält der Betreiber einen Überblick über den Zustand der Komponenten. <u>Wann wird getestet?</u> • Der Administrator prüft laufend und meist automatisiert die Funktion der Geräte mit Hilfe eines NMS-Systems. Die Systemdokumentation ist vom Administrator laufend aktuell zu halten. • Der Stand der Datensicherung, die Integrität der Konfigurationsdateien und weitere Daten zur Konfiguration sollten vom Administrator regelmäßig (wöchentlich) geprüft werden. • Scans mit der Hilfe von Sicherheits-Tools sollten nach Installation regelmäßig (monatlich) durch den Administrator vorgenommen werden. Die Ergebnisse sind zu prüfen und zu archivieren. • Die Prüfung der Einhaltung von Sicherheitsrichtlinien muss regelmäßig erfolgen (z. B. jährlich im Rahmen von Sicherheits- oder Grundschutzaudits). <u>Wer testet?</u> • Der Administrator sollte laufend Prüfungen durchführen (Funktion der Komponenten, Stand der Datensicherung, Integrität der Konfigurationsdateien, Scans, etc.). • Die Einhaltung von Sicherheitsrichtlinien bzw. von Sicherheitsmaßnahmen im Rahmen von Sicherheits- bzw. Grundschutzaudits darf nicht durch den Administrator geprüft werden, sondern hat abhängig vom etablierten Sicherheitsmanagementprozess durch einen Auditor, IT-Sicherheitsbeauftragten oder Revisor zu erfolgen.

		• Welche Informationen bilden die Grundlage der Kontrolle? • Sicherheitsrichtlinie für Loadbalancer • Protokolldateien von Loadbalancer • Systemdokumentation (siehe M 2.281 Dokumentation der Systemkonfiguration von Loadbalancern) • IT-Sicherheitskonzept • IT-Grundschutz-Kataloge • Ergebnisse von durchgeführten Scans • Überprüfung der Konfiguration • Bei der Einrichtung der Loadbalancer sind alle Default-Einstellungen zu prüfen und falls notwendig zu modifizieren. Hierbei werden beispielsweise nicht benötigte Dienste deaktiviert und Voreinstellungen den betrieblichen und sicherheitstechnischen Anforderungen angepasst. Eine Erläuterung der hierfür notwendigen Schritte findet sich in M 4.201* Sichere lokale Grundkonfiguration von Loadbalancern und M 4.202 Sichere Netz-Grundkonfiguration von Laodbalancern. Die Umsetzung der Vorgaben zum Umgang mit Default-Einstellungen ist im Rahmen von regelmäßigen Audits zu überprüfen. Hierdurch können versehentliche oder vorsätzliche Veränderungen festgestellt und die Umsetzung von aktuellen Empfehlungen der Hersteller verifiziert werden. Dies kann ausgehend von der für jeden Gerätetyp beziehungsweise für jede Betriebssystemversion zu erstellenden Installationsanleitung erfolgen und sollte am jeweiligen Gerät verifiziert werden. Hierbei ist jedoch zu beachten, dass Betriebssystem-Kommandos bei manchen Herstellern nicht alle Default-Einstellungen anzeigen. Aus diesem Grund empfiehlt es sich, separate Software-Tools einzusetzen, um eine vollständige Analyse durchzuführen.
M 2.283 *	(B)	**Software-Pflege auf Loadbalancern** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Jeglicher Betrieb von Software macht es notwendig, Betriebssystem und Konfiguration regelmäßig zu überprüfen und zu pflegen. Loadbalancer können hiervon nicht ausgenommen werden, um beispielsweise funktionale Erweiterungen zu ermöglichen, Softwarefehler zu

		beheben und Performance und Sicherheit zu verbessern. Dabei ist zu beachten, dass in der Praxis zur Pflege des Betriebssystems bei Loadbalancern ein kompletter Austausch der Betriebssystemsoftware erforderlich ist. Das Einspielen von Updates oder Patches ist in vielen Fällen nicht möglich. Wie bei allen Konfigurationsänderungen ist mit angemessener Sorgfalt vorzugehen, da eine unsachgemäße Durchführung Beeinträchtigungen der Funktion und der Sicherheit der Geräte zur Folge haben kann. Insofern gehört zur sorgfältigen Planung einer Änderung immer auch eine Fallback-Strategie. Einspielen neuer Software Bei der Vorbereitung von Updates sind folgende Punkte zu beachten: • Es muss ein geeignetes Zeitfenster vorgesehen werden. Der benötigte Aufwand sollte nicht unterschätzt werden und vorsichtshalber eine ausreichende Down-Time eingeplant werden. • Die vom Hersteller beigefügten Hinweistexte (Release Notes) des neuen Release sind sorgfältig zu lesen. • Bei neuen Softwareversionen sind eventuell einzelne Features nicht mehr enthalten oder funktionieren nicht korrekt. Manchmal ändern sich auch Defaulteinstellungen. • Neue Versionen einer Firmware oder eines Betriebssystems müssen vor der Inbetriebnahme sorgfältig getestet werden, um die volle Funktionalität sicher zu stellen. Neue Firmware oder Betriebssysteme sind unter Umständen weniger performant, beispielsweise wegen zusätzlicher Features oder höherem Speicherbedarf. Dies kann zu Problemen führen, wenn ein Loadbalancer bereits vor dem Upgrade an der Auslastungsgrenze betrieben wurde. Bei der Durchführung von Updates sollten folgende Schritte durchgeführt werden: • Beschaffung des Updates aus vertrauenswürdiger Quelle. Normalerweise sollten Updates nur vom Hersteller bezogen werden. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, so sollten die Prüfsummen oder Signaturen überprüft werden (siehe auch M 2.273* Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates und M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen). • Überprüfung der Integrität und Funktion des Updates

		• Trennung des Gerätes vom produktiven Netz oder Deaktivierung aller Schnittstellen • Nach Möglichkeit Sicherung der bestehenden Konfiguration und des Betriebssystems • Einspielen des Updates • Test • Re-Aktivierung des Gerätes im Netz Änderung der Konfiguration Konfigurationsänderungen können sowohl direkt am Gerät an der System-Konsole (online) als auch auf einem eigenen Management-Rechner mit einem entsprechenden Konfigurationsprogramm oder einem Texteditor (offline) vorgenommen werden. Beide Vorgehen haben Vor- und Nachteile, generell ist jedoch die Offline-Konfiguration zu bevorzugen, da die Syntax zeitnah überprüft werden kann. In jedem Fall muss der Administrationsrechner, auf dem die Offline-Konfiguration vorgenommen wird beziehungsweise auf dem die Konfigurationsdaten gehalten werden, vor unbefugtem Zugriff besonders geschützt werden.
M 2.302*	(Z)	**Loadbalancer und Hochverfügbarkeit** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Ein Loadbalancer stellt eine Schnittstelle zwischen den Client-Anfragen für die konfigurierten Dienste und den bereitstellenden Servern dar. Somit stellt der Loadbalancer eine mögliche Bruchstelle für alle lastverteilten Dienste einer Organisation dar. Daher werden an die Verfügbarkeit von Loadbalancern häufig hohe Anforderungen gestellt. Es gibt verschiedene Möglichkeiten, die Verfügbarkeit von Komponenten eines Loadbalancers zu steigern: Cold-Standby Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht in Betrieb ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und integriert werden. Hot-Standby Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem (meist mit der gleichen Konfiguration wie das im Regelbetrieb befindliche Sys-

		tem) bereit. Dieses läuft aber ständig parallel mit, wobei eine Komponente die andere überwacht. Bei einer Fehlfunktion kann dann das Ersatzsystem unmittelbar die Funktion des Wirksystems übernehmen. Dies kann automatisiert erfolgen oder auch nach Benutzerinteraktion. Eine Benutzerinteraktion kann verhindern, dass eine Umschaltung auf das Hot-Standby-System - die zusätzliche Komplikationen mit sich bringen kann - bei extrem kurzen Ausfällen erfolgt. Verwendung von Layer-3 Redundanzprotokollen Da Loadbalancer in typischen Einsatzszenarien Routingfunktionen übernehmen und somit Gateway für die konfigurierten Subnetze darstellen, kann beim Einsatz von 2 Loadbalancern unter Verwendung der Protokolls VRRP (Virtual Router Redundanc Protokoll) ein Single Point of Failure vermieden werden. Je nach Implementierung dieses Protokolls können Active-Standby oder Active-Active Konfigurationen realisiert werden. Dabei erfolgt die Auswahl des VRRP-Masters anhand der aktuellen Priorität für ein bestimmtes Interface. Weitergehende herstellerspezifische Implementierungen erlauben u.a. die dynamische Veränderung der Prioritäten anhand der Anzahl der aktiven Interfaces, aktiven Ports oder weiterer L4 Parameter. Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden.
M 4.204*	(C)	**Sichere Administration von Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Es gibt unterschiedliche Zugriffsmöglichkeiten, um Loadbalancer zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, Loadbalancer in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration praktisch nicht gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden, und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden. Alle nicht verwendeten Administrationsschnittstellen sollten deaktiviert werden. Im Folgenden werden einige Punkte beschrieben, die bei der Administration beachtet werden sollten.

		Zusätzlich sollte wenn möglich der Administrationszugriff durch die Einrichtung von Access Control Lists (ACLs) eingeschränkt werden (siehe auch M 5.111* Einrichtung von Access Control Lists auf Loadbalancer). Remote-Administration Eine Vielzahl von aktiven Netzkomponenten bietet die Möglichkeit der Remote-Administration mit Hilfe des Dienstes Telnet. Die Nutzung von Telnet birgt allerdings die Gefahr des Ausspähens von Authentisierungsdaten, da sämtliche Daten im Klartext übertragen werden und somit der Datenverkehr inklusive des Benutzernamens und Passwortes mitgelesen werden kann (siehe auch G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen). Oft wird zur Remote-Administration auch SNMP verwendet. Die Varianten SNMPv1 und SNMPv2 bieten ebenfalls keine ausreichenden Möglichkeiten zur Absicherung der Kommunikation. Erst SNMPv3 bietet Sicherheitsmechanismen, die einen Einsatz auch außerhalb abgeschotteter Administrationsnetze erlauben. Bei Remote-Zugriff auf Loadbalancer muss in jedem Fall eine Absicherung der Kommunikation erfolgen. Dies kann beispielsweise durch die Nutzung des Dienstes SSH anstatt Telnet (siehe M 5.64 Secure Shell) oder durch die Schaffung eigener LAN-Segmente, die ausschließlich für Administrationszwecke genutzt werden, erreicht werden (siehe Abschnitt Administrationsnetz). Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden. Webserver Viele Geräte bieten die Möglichkeit, Administrationsarbeiten mit Hilfe des Dienstes HTTP über ein Browser-Interface durchzuführen. Auf dem Loadbalancer ist in diesem Fall ein HTTP-Server gestartet, der Zugriff erfolgt von beliebigen Clients über Web-Browser. Die Standardeinstellungen für den Zugriff auf das Web-Interface sind nicht bei allen Herstellern einheitlich. Idealerweise sollte der Zugriff in der Grundeinstellung deaktiviert sein, es ist aber auch möglich, dass dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen verwendet werden kann. Dies ist bei der Inbetriebnahme der Geräte zu prüfen, gegebenenfalls muss die Konfiguration entsprechend geändert werden. Wie bei der Nutzung des Dienstes TELNET wird auch beim HTTP der

		Benutzername und das Passwort im Klartext übertragen. Zudem ist eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server der unterschiedlichen Hersteller ausnutzen. Daher wird von der Nutzung des HTTP-Dienstes für Administrationszwecke dringend abgeraten. Der HTTP-Server sollte nach Möglichkeit bei der Erstkonfiguration des Systems deaktiviert werden, sofern der Zugriff nicht über ein gesondertes Management-Netz erfolgt. Manche Geräte bieten zusätzlich zum Zugriff über HTTP auch die Möglichkeit, über HTTPS auf das Web-Interface zuzugreifen. Sofern diese Möglichkeit besteht, sollte HTTPS in jedem Fall der Vorzug vor HTTP gegeben werden. Bei der Nutzung des Web-Interfaces muss außerdem beachtet werden, dass oft nicht alle Konfigurationseinstellungen auf diesem Weg zugänglich sind. Administrationsnetz (Out-of-Band-Management) Um den Risiken bei der Remote-Administration entgegen zu wirken, bieten einige Geräte die Möglichkeit, einen eigenen logischen Port (Management-Interface) zur Administration zu konfigurieren. Dieser Port sollte einem VLAN bzw. Subnetz zugeordnet werden, welches ausschließlich für administrative Zwecke verwendet wird (Out-of-Band-Management) und dem ausschließlich Management-Interfaces angehören. Das Management-Netz sollte komplett von anderen Teilen des Netzes getrennt werden. Dadurch werden Schwachstellen wie unverschlüsselt übertragene Anmeldeinformationen bei den für administrative Aufgaben zur Anwendung kommenden Protokollen wie TELNET oder die veralteten SNMP-Varianten kompensiert. Access Control Lists (ACLs) sind so zu konfigurieren, dass der Zugriff auf das Management-Interface nur der Management-Station erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren. Netzmanagement-Systeme Aktive Netzkomponenten werden normalerweise in ein zentrales Netzmanagement-System eingebunden. Zusätzlich zum vorigen Abschnitt müssen in diesem Fall die Sicherheitsmaßnahmen, die im Baustein B 4.2 Netz- und Systemmanagement beschrieben sind, beachtet werden. Zentraler Authentisierungsserver An Stelle lokal auf dem Gerät zu konfigurierender Zugriffs- und Rechtekontrolle kann dies auch über einen zentralen Server erfolgen. Bei großen Umgebungen mit einer hohen Anzahl von aktiven Netzkomponenten ist die lokale Konfiguration nur bedingt praktikabel. Der

		Aufwand für die Administration und für viele parallel zu pflegende Berechtigungen ist dann sehr hoch. Auf dem zentralen Server werden dabei einheitlich alle Zugriffe und Berechtigungen verwaltet. Die sensitiven Daten sind nicht mehr auf den Geräten selbst gespeichert und müssen nicht einzeln gepflegt werden. Stattdessen sind alle Informationen verschlüsselt in einer Datenbank abgelegt und lassen sich übersichtlich verwalten. Ein solcher Server bietet zudem erweiterte Möglichkeiten zur Protokollierung, beispielsweise können Anzahl und Zeitpunkt von Einwahl- oder Zugriffsvorgängen und übertragene Datenmengen dokumentiert werden. Beispiele hierfür sind RADIUS und TACACS+ (Terminal Access Controller Access Control System). Die Authentisierung sollte in komplexen Netzen mit einer Vielzahl von aktiven Netzkomponenten durch einen zentralen Authentisierungsserver abgesichert werden. Für den Fall, dass kein Authentisierungsserver genutzt werden kann (beispielsweise beim Ausfall des Servers oder bei Netzproblemen), sollte trotzdem ein lokaler Zugriff konfiguriert sein. Dieser ist durch ein nur für diesen Zweck zu nutzendes Passwort abzusichern. Für lokale Zugänge, die nicht eigens für den Fall eingerichtet wurden, dass der Authentisierungsserver nicht zur Verfügung steht, sollten der Authentisierungsserver nach Möglichkeit genutzt werden, da ansonsten die Benutzer, die sich lokal anmelden, die zentrale Autorisierung und Überwachung umgehen. <u>Berechtigungsverwaltung für Benutzerkonten und Systemkommandos</u> Die Berechtigungsverwaltung kann je nach Hersteller auf unterschiedlichen Ebenen und mit unterschiedlichen Graden der Granularität erfolgen. Bei der Berechtigungsverwaltung von Systemkommandos können Kommandos, die nur bestimmten Nutzern oder Gruppen zugänglich sein sollen, in einer Berechtigungsstufe zusammengefasst bzw. dieser zugeordnet werden. <u>Zuordnung von Systemkommandos zu Berechtigungsstufen</u> Der Zugriff auf eine Berechtigungsstufe wird durch ein Passwort abgesichert. Ein Nutzer muss für den Zugriff auf ein entsprechend abgesichertes Systemkommando zunächst in die Berechtigungsstufe wechseln und das zugehörige Passwort eingeben. Dann ist er in der Lage, alle dieser Stufe zugeordneten Kommandos auszuführen. Die Berechtigungsvergabe für Benutzerkonten erfolgt, indem der Nutzer einer Berechtigungsstufe zugeordnet wird. Generell sollte gelten, dass jedem Nutzer nur die minimal notwendigen Berechtigungen zugeteilt werden. Somit lassen sich analog der folgenden Beispiele unterschiedliche Rollen definieren:

		• Ein Benutzer-Account dient dazu, die Statusinformationen und Statistiken des Geräts einzusehen. Änderungen der Konfiguration sind nicht möglich. • Der Server-Loadbalancer-Operator-Account erlaubt das Management der Content Server sowie deren Auslastung. Neben der Berechtigung alle Geräteinformationen und Statistiken einzusehen, darf er auch die Server, welche an dem Loadbalancing teilnehmen, aktivieren oder auch deaktivieren. • Der Layer 4-Operator-Account erlaubt neben den Rechten des SLB-Operators auch Trafficmanagement auf den Verbindungen, die zu gemeinsam genutzten Internetdiensten führen. • Der Operator-Account erlaubt das Managen aller Funktionen des Loadbalancers. In Erweiterung der Rechte des SLB-Operators darf er einzelne Ports oder auch den gesamten Loadbalancer zurücksetzen. • Der Server-Loadbalancer -Administrator Account erlaubt die Konfiguration und das Management der Content Server sowie deren Auslastung. Zusätzlich zu den SLB-Operator Funktionen kann er Parameter für das Loadbalancing ändern. Er darf jedoch keine Filter konfigurieren. • Der Layer 4-Administrator Account erlaubt die Konfiguration und das Management der auf den Verbindungen, die zu gemeinsam genutzten Internetdiensten führen. Zusätzlich zu den SLB-Administrator Funktionen kann er alle Parameter für das Loadbalancing ändern und auch Filter konfigurieren. • Der Administrator- Account ist für die umfassende Kontrolle inklusive Sicherheitseinstellungen, Zugriffspassworte und Web-basierte Managementzugriffe vorgesehen. Ein Benutzer ist somit nach seiner Anmeldung am Gerät automatisch einer Berechtigungsstufe zugeordnet, alternativ muss er nach der Anmeldung dediziert die zu nutzende Berechtigungsstufe und das zugehörige Passwort eingeben. Für sicherheitskritische Rollen sollte stets eine Absicherung des Zugriffs über einen zentralen Authentisierungsserver eingerichtet werden. Bei der Erstellung des Rechte- und Rollenkonzepts für die Administration der aktiven Netzkomponenten müssen die Möglichkeiten der einzelnen Systeme in Betracht gezogen werden. Wie fein die Berechtigungsstufen im Einzelfall unterschieden werden, sollte unter Berücksichtigung von Einsatzzweck und Schutzbedarf festgelegt wer-

		den. Als Faustregel kann dabei gelten: "So fein wie nötig, so einfach wie möglich." Zu grobe Unterteilungen bieten keine angemessene Sicherheit, andererseits können zu feine Unterteilungen die Effizienz der Arbeit beeinträchtigen und bringen die Gefahr von Fehlern mit sich. Passwortverschlüsselung Loadbalancer sollten die Möglichkeit unterstützen, Passwörter verschlüsselt in Konfigurationsdateien abzulegen (siehe auch M 2.280* Kriterien für die Beschaffung und geeignete Auswahl von Loadbalancern. Die Verschlüsselung von Passwörtern ist insbesondere dann wichtig, wenn Konfigurationsdateien über das Netz übertragen oder in zentralen Servern gespeichert werden. Wenn das Gerät die Passwortverschlüsselung unterstützt, sollte diese Funktion unbedingt genutzt werden. Dabei sollte das Verschlüsselungsverfahren berücksichtigt werden, da einige Geräte unterschiedliche Verfahren unterstützen. Insbesondere bei älteren Betriebssystemen werden noch schwache Verschlüsselungsverfahren angewendet, die eventuell aus Gründen der Kompatibilität auch in neueren Versionen noch unterstützt werden. Hier sollte bei einer Migration auf ein neues Gerät oder eine neue Betriebssystemversion geprüft werden, ob die neuere Version stärkere Verschlüsselungsverfahren unterstützt. Zudem bestehen für alle Geräte Prozeduren, die es zwar nicht ermöglichen, verschlüsselte Passworte wieder lesbar zu machen, die aber das Rücksetzen von Passwörtern durchführen. Einige Dienste können nicht durch eine Passwort-Verschlüsselung abgesichert werden. Hierzu gehören SNMPv1 und SNMPv2, RADIUS und TACACS+. Die Passwörter der letztgenannten Dienste sollten somit immer einmalig sein, für keinen weiteren Dienst verwendet und regelmäßig geändert werden. SNMPv1 und SNMPv2 sollten allenfalls in Verbindung mit Out-of-Band-Management (siehe oben: Administrationsnetz) genutzt werden und möglichst durch SNMPv3 ersetzt werden. Session-Timeouts Sämtliche Zugriffsarten können durch die Vergabe von Passwörtern geschützt werden. Diese Absicherung kann jedoch wirkungslos werden, wenn Sessions unbeaufsichtigt sind, beispielsweise wenn ein angemeldeter Administrator seinen Rechner verlässt und dabei vergisst, die Session zu beenden oder die Bildschirmsperre zu aktivieren. Aus diesem Grund ist es empfehlenswert, Time-outs einzu-

		richten, um Verbindungen nach einem definierten Zeitraum ohne Nutzeraktivität zu beenden oder zu sperren. Dabei sollte eine Timeout-Zeit von 10 Minuten nicht überschritten werden.
M4.205*	(C)	**Protokollierung bei Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Loadbalancer bieten in der Regel Möglichkeiten zur Protokollierung. Die Auswertung dieser Informationen ermöglicht die Beurteilung der korrekten Funktion des Geräts und das Erkennen von Angriffsversuchen. Mit Hilfe der Protokollierungsinformationen kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden. Daher sollte die Protokollierung immer genutzt und sorgfältig eingerichtet werden. Die sorgfältige Konfiguration ist besonders wichtig, da nur bei einer sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert werden können. Hierzu gehören vor allem das Erkennen abgewiesener Zugriffsversuche und Änderungen der Konfiguration. Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (M 2.110 Datenschutzaspekte bei der Protokollierung). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden. Folgende Informationen sollten nach Möglichkeit protokolliert werden: • Konfigurationsänderungen • Reboots • Systemfehler • Statusänderungen pro Interface, System und Netzsegment • Login-Fehler (zumindest dann, wenn sie wiederholt auftreten) • Verstöße gegen ACL-Regeln (abgewiesene Zugriffsversuche) Insbesondere der letzte Punkt sollte für jede ACL aktiviert werden, um alle fehlgeschlagenen Versuche zu erfassen und falsch oder nicht korrekt konfigurierte Regeln erkennen zu können.

		Neben einer geeigneten Speicherung der Informationen kommt der möglichst zeitnahen Auswertung besondere Bedeutung zu. Hierfür existieren unterschiedliche Ausgabemöglichkeiten, die abgestimmt auf die individuellen Bedürfnisse auch in Kombination miteinander angewendet werden können: SNMP Herstellerabhängig lassen sich auf Loadbalancern für eine Vielzahl von Ereignissen SNMP-Nachrichten generieren, die von einem bestehenden Netzmanagementsystem erkannt, angezeigt und verarbeitet werden können. Dies ermöglicht eine automatisierte Auswertung. Ausgabe an der Konsole Die Ausgabe der Protokollierung an der Konsole erlaubt keine dauerhafte Speicherung kann daher lediglich eine Ergänzung zu anderen Methoden darstellen. Zentraler Authentisierungsserver Bei der Nutzung eines zentralen Authentisierungsservers, zum Beispiel mittels TACACS+ oder RADIUS, kann die dort implementierte Protokollierung (Accounting) genutzt werden, um Nutzeraktivitäten zu dokumentieren. Syslog Die Protokollierungsinformationen können über das Netz auf einen eigenen syslog-Server übertragen werden. Dies dient der zentralen Sammlung und Archivierung der Protokollierungsinformationen, da auf den Netzkomponenten oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Dadurch können an einer zentralen Stelle relevante Informationen erfasst und ausgewertet werden. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokollierungsinformationen vom Angreifer nicht verändert oder gelöscht werden können. Die Übertragung zum syslog-Server erfolgt meist unverschlüsselt über TCP oder UDP, so dass ein Mithören auf dem Übertragungsweg möglich ist. Somit kann durch das Versenden von Informationen aus dem internen Netz die Vertraulichkeit der im internen Netz vorhandenen Informationen gefährdet werden. Daher sollte überlegt werden, die Übertragung über ein eigenes Netz (Administrationsnetz) abzuwickeln. NTP Alle Protokollierungsinformationen sollten mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbesondere bei der Analyse von versuchten oder erfolgten

		Angriffen, sichergestellt. Aus diesem Grunde sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen. Dazu sollte in Erwägung gezogen werden, im internen Netz einen eigenen Zeit-Server einzurichten, der beispielsweise auf einem eigenen Rechner angesiedelt ist, der mit einer Funkuhr verbunden ist. Alternativ kann ein geeigneter Rechner als NTP-Proxy dienen und die Zeitinformation seinerseits per NTP von einem Zeit-Server im Internet (beispielsweise von der Physikalisch-Technischen Bundesanstalt (PTB)) bezieht. Im Zweifelsfall sollte die erste Lösung (interner Zeitserver mit Funkuhr) bevorzugt werden, insbesondere in Netzen mit hohem Schutzbedarf. Keinesfalls sollten alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.
M 5.70*	(A)	**Adressumsetzung – NAT(Network Address Translation)** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Network Address Translation (NAT) ist ein Mechanismus, bei dem eine aktive Netzkomponente (in der Regel ein Router oder Loadbalancer) bei der Weiterleitung eines Paketes die IP-Adresse des Paketes verändert. Der Loadbalancer speichert in einer Tabelle die Zuordnung der internen Adresse und des internen Quell-Ports zur externen Adresse, Zielport und dem Port, den der Loadbalancer selbst für das veränderte Paket gewählt hat und setzt die Antwortpakete entsprechend um. NAT kann zu verschiedenen Zwecken verwendet werden: • NAT kann verhindern, dass anhand der IP-Adressen im lokalen Netz auf dessen Struktur rückgeschlossen wird, denn vom externen Netz aus ist nur die IP-Adresse des NAT-Gateways sichtbar. Dies verhindert gleichzeitig, dass Angreifer von außen direkt einzelne Rechner im internen Netz attackieren können. • Im lokalen Netz werden oft mehr IP-Adressen benötigt, als offiziell registriert sind. Bei Verwendung eines NAT-Gateways wird für jedes Netz nur eine einzige offizielle IP-Adresse zwingend benötigt, die internen Adressen können beliebig gewählt werden. • Beim Aufbau eines internen Netzes sollten interne Adressen unbedingt nur aus den Bereichen gewählt werden, die offiziell

für solche Zwecke vorgesehen sind (siehe RFC 1918 - Address Allocation for Private Internets). Diese Adressen werden im "allgemeinen Internet" nicht geroutet und müssen daher am Gateway zum Internet in eine offiziell zugeteilte IP-Adresse umgesetzt werden.

- Gelegentlich wurden beim Aufbau eines internen Netzes einfach beliebige IP-Adressen verwendet. Beim Anschluss eines solchen Netzes an das Internet können diese bisher verwendeten IP-Adressen dann oft nicht benutzt werden, da der betreffende Adressbereich an andere Institutionen vergeben wurde. Um nicht alle Rechner neu konfigurieren zu müssen, kann eine Adressumsetzung von den internen zu den offiziell registrierten externen Adressen sinnvoll sein. Allerdings werden in diesem Fall oft Probleme bei der Namensauflösung eintreten und die Rechner, denen die intern verwendeten Adressen im Internet zugeordnet sind, werden aus dem internen Netz nicht erreichbar sein. Auch bei einem Wechsel des Internet-Providers kann dieser Fall eintreten.
- Beim Zusammenschluss zweier Netze, bei denen IP-Adressen aus den Bereichen des RFC-1918 gewählt wurden, kann ebenfalls eine Adressumsetzung notwendig werden, wenn in beiden Netzen dieselben Adressen verwendet wurden.

Eine Umsetzung der internen in eine oder mehrere offiziell registrierte IP-Adressen und umgekehrt erfolgt über eine Adressumsetzungskomponente. Auch Proxies verfügen über eine implizite Adressumsetzung, da der Proxy extern nur seine offizielle Adresse verwendet und die Datenpakete an die jeweiligen internen Rechner weiterleitet.

<u>Zugriff von außen bei NAT</u>

Für einen Verbindungsaufbau von außen (z. B. bei Anfragen an einen Web-Server) werden am NAT-Gateway alle Pakete, die an einen bestimmten Port gerichtet sind, umgesetzt und an einen entsprechenden Port des Servers weitergeleitet. Dieser Mechanismus wird auch als "Destination NAT" oder "Port-Forwarding" bezeichnet. Mit den Antwortpaketen des Servers verfährt das NAT-Gateway analog.

<u>NAT in Verbindung Loadbalacing</u>

Bei einer Verbindungsanfrage von außen (z.B. Anfragen an einen Web- oder LDAP-Server) an ein lastverteiltes Serversystem gerichtet ist, kann sich der Client nur die sogenannte virtuelle IP-Adresse des Zielsystems bzw. den ihm zugeordneten Namen wenden. Der Loadbalancer nimmt diese Anfrage entgegen und vermerkt in seiner Sitzungstabelle, die Quell-IP-Adresse und den Quell-Port sowie die Ziel-IP-Adresse (Virtuelle-IP-Adresse) und den Ziel-Port resp. Dienst. An-

		schließend weist der Loadbalancer diese Anfrage nach den vorgegebenen Loadbalancing-Parametern einem konkreten Server zu und ersetzt die Ziel-IP-Adresse (Virtuelle-IP) durch die IP-Adresse des realen Servers. Dabei spielt es keine Rolle, ob sich die realen Server mit ihrer IP-Adresse im gleichen Subnetz befinden oder nicht. Der Austausch der Ziel-IP-Adresse wir ebenfalls in der Sitzungstabelle vermerkt und Grundlage für die Zuordnung des Antwortpaketes des Servers, welches er an den Loadbalancer zurücksendet. Dieser tauscht in der Antwort an den Client die reale IP-Adresse des Servers wieder gegen die Virtuelle-IP-Adresse aus. Da ein Loadbalancer bei der Lastverteilung von Anwendungen immer auch ein NAT durchführt, können die realen Server auch mit RFC-1918 Adressen im Internet Dienste zur Verfügung stellen, solange die Virtuelle-IP eine registrierte Adresse ist. Dabei kann auf die Server selbst vom Internet aus nicht zugegriffen werden.

2.3.5 Aussonderung

M 2.167	(B)	**Sicheres Löschen von Datenträgern** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Verantwortlich für Umsetzung: Fachverantwortliche, Administrator, Benutzer • Häufige Fehleinschätzungen Nahezu jeder wird schon erlebt haben, wie schnell ein Datenverlust eintreten kann, beispielsweise durch falsche Lagerung eines Datenträgers. Schon bei einer Festplatte, die "nur" feucht geworden ist, oder einer CD-ROM, die "nur" zu warm wurde, weil sie zu lange am Fenster lag, ist häufig kein Datenzugriff mehr möglich. Daher sind viele Anwender der Meinung, dass Informationen auf Datenträgern, die durch Feuer, Hitze-Einwirkung oder Wasserschäden beschädigt wurden, restlos vernichtet sind. Diese Informationen lassen sich allerdings - stark abhängig vom Grad der Beschädigung - teilweise von Datenrettungsfirmen und entsprechend ausgestatteten Organisationen erfolgreich wiederherstellen. Defekte Festplatten können unter Umständen durch den Austausch von Bauteilen wieder funktionstüchtig gemacht oder durch spezielle Geräte ausgelesen werden. Auch etliche "Hausmittel" zum Löschen von magnetischen Datenträgern, wie die Behandlung mit Mikrowellen oder mit sehr starken Magneten, die nicht für diesen speziellen Einsatzzweck vorgesehen sind, sind ungeeignet. Um Informationen auf Datenträgern sicher zu löschen, müssen deshalb einige Hinweise beachtet und ein Verfahren gewählt werden, das

		für das jeweilige Medium, für den Schutzbedarf der Informationen und für den konkreten Anwendungsfall geeignet ist. • Arten von Speichermedien und Datenträgern Speichermedien und Datenträger lassen sich zunächst in analoge Speichermedien, wie Papier oder Mikrofilm, einerseits und digitale Speichermedien andererseits unterscheiden. Letztere lassen sich im Wesentlichen einteilen in - magnetische Speichermedien wie Festplatten, Disketten, Wechselplatten, Zip-Disketten, Magnetbänder, - optische Speichermedien (z. B. CD, DVD), - elektronische Speichermedien (z. B. Flash-Speicher oder Flash-Karten, wie USB- bzw. Memory-Sticks oder andere elektronische Speicherkarten). Soweit nicht weiter unterschieden wird, gelten die folgenden Empfehlungen für alle Arten von Datenträgern. • Vorgehensweisen und Methoden Damit gespeicherte Daten nicht in falsche Hände geraten können, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger zu löschen oder zu vernichten. Bevor Datenträger wieder verwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden, z. B. durch vollständiges Überschreiben. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen. Auch der Empfänger eines Datenträgers muss nach dem Empfang prüfen, ob der Schutzwert der Daten ein sofortiges Löschen des Datenträgers erfordert, nachdem die Daten auf ein anderes IT-System übertragen wurden. Es gibt verschiedene Methoden, um Informationen auf Datenträgern zu löschen. Welche Methode gewählt werden sollte, hängt hierbei wesentlich vom Schutzbedarf der zu löschenden Daten ab, aber natürlich auch von der Art der Datenträger. Im Folgenden sind Hinweise und Empfehlungen für die wichtigsten Methoden zum Löschen und Vernichten von Datenträgern aufgeführt. • Löschkommandos Löschkommandos sind vom Betriebssystem zur Verfügung gestellte Befehle und Funktionen, um Dateien oder Verzeichnisse zu löschen. Bei der Benutzung von Löschkommandos ist zu beachten, dass dabei in der Regel nicht tatsächlich die Datei-Informationen gelöscht werden, sondern nur der Verweis auf diese Informationen im "Inhaltsverzeichnis" des Datenträgers. Die Datei ist weiterhin vorhanden. Es gibt Methoden und Programme, mit denen die gelöscht geglaubten Informationen wiederhergestellt werden können. Von dieser Methode ist daher abzuraten, wenn sichergestellt sein muss, dass die Daten nicht rekonstruiert werden können. • Überschreiben einzelner Dateien

		Neben den im Umfang der gebräuchlichen Betriebssysteme vorhandenen Löschkommandos gibt es auch zusätzliche Werkzeuge, um einzelne Dateien zu überschreiben. Mit diesen so genannten Wipe-Tools lassen sich einzelne Dateien durch vollständiges Überschreiben mit geeigneten Datenmustern vollständig löschen. Dabei ist allerdings darauf zu achten, dass Informationen aus Dateien häufig teilweise oder sogar vollständig rekonstruierbar sind, obwohl die Dateien mit Wipe-Tools gelöscht wurden. Hauptsächlich liegt das daran, dass Kopien dieser Daten während der Verarbeitung temporär auf Datenträgern abgelegt werden. Restinformationen können beispielsweise aus folgenden Quellen gewonnen werden: - vom Betriebssystem bzw. Anwendungsprogramm erstellte und wieder gelöschte Zwischendateien (Cache-Dateien) oder temporäre Dateien, - automatisch von einem Programm angelegte Sicherungskopien, wie diese beispielsweise von Office-Programmen häufig angelegt werden, - Auslagerungsdateien, - Daten-Fragmente, die unter Windows-Betriebssystemen in der Registry oder in Index-Datenbanken vorhanden sein können, File-Slack (File-Slack oder Datenversatz bezeichnet das bei einigen Betriebssystemen übliche Abspeichern von "Auffülldaten" in unallozierte Bereiche von Datenträgern) bzw. Cluster-Tip-Areas. Auf die Verarbeitung dieser Daten durch das Betriebssystem oder Anwendungsprogramm haben Administratoren oder Benutzer oft nur sehr geringen Einfluss. Auch Programme, die Wipe-Techniken verwenden, haben keine volle Kontrolle über alle diese Datenspuren. Daher muss der komplette Datenträger gelöscht oder ein anderes sicheres Löschverfahren gewählt werden, um sicherzustellen, dass sich keine weiteren Kopien der Informationen auf dem Datenträger befinden (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*). An dieser Stelle wird noch einmal darauf hingewiesen, dass bei den normalen Löschkommandos des Betriebssystems in der Regel keine Wipe-Techniken zum Einsatz kommen. Weitere Hinweise hierzu finden sich im Abschnitt "Löschkommandos". • Formatieren Elektronische Datenträger können durch Formatieren zur Aufnahme von Daten vorbereitet werden. Bei Festplatten wird zwischen Low-Level-Formatierung, bei der Spuren und Sektoren auf der Platte neu erzeugt werden, und der logischen oder High-Level-Formatierung, die durch das Betriebssystem erfolgt, unterschieden. Eine High-Level-Formatierung ist als sicheres Löschverfahren unge-

		eignet, da dabei lediglich die Dateisystemstruktur neu angelegt wird. Für Festplatten konnte früher durch den Anwender eine sogenannte *Low-Level-Formatierung* durchgeführt werden, bei der die magnetischen Grundstrukturen neu geschrieben wurden. Bei modernen Festplatten kann dies in der Regel nur der Hersteller vornehmen. Stattdessen stellen einige Festplatten-Hersteller Tools zur Verfügung, mit denen auch eine vollständige Löschung der Festplatte vorgenommen werden kann (sogenannter *Zero-Fill*). Über die Zuverlässigkeit der Löschung durch Low-Level-Formatierungen oder Zero-Fills kann jedoch keine Aussage getroffen werden. Von der Nutzung eines dieser Mechanismen als Löschverfahren wird deshalb abgeraten. Wenn dennoch eine Low-Level-Formatierung oder ein Zero-Fill durchgeführt werden soll, sollte vorher geklärt werden, ob dadurch die Garantie für die Festplatte verloren geht. Für wiederbeschreibbare CD-ROMs (CD-RW), Disketten oder ähnliche Datenträger muss beachtet werden, dass eine schnelle Formatierung die Daten nicht löscht. Eine komplette Löschung ist daher notwendig. Weitere Hinweise hierzu finden sich im Abschnitt "Vernichtung von Datenträgern". • Löschgeräte für magnetische Datenträger Löschgeräte dienen dazu, schutzbedürftige Daten, die auf magnetischen Datenträgern gespeichert sind, so zu vernichten, dass die Datenträger anschließend wiederverwendet werden können. Löschgeräte (Degausser) für magnetische Datenträger verfügen über einen starken Gleichfeld- oder Wechselfeldmagneten. Beim Löschen mit einem Löschgerät werden die Datenträger vom Magnetfeld des Gerätes durchflutet ("Durchflutungslöschen"). Da es sich beim Löschen mit Löschgeräten ausschließlich um eine magnetische Einwirkung handelt, können Löschgeräte auch nur bei magnetischen Datenträgern wie Magnetbändern, Disketten und Festplatten verwendet werden. Durch das Magnetfeld eines Löschgerätes werden die aufgezeichneten magnetischen Domänen auf den Datenträgern zerstört. Bei Verwendung eines geeigneten Löschgerätes ist nach dem Löschen auf dem Datenträger keine Information mehr vorhanden. Der Vorteil beim Löschen mit einem Löschgerät besteht darin, dass mit geringem Zeitaufwand der gesamte Datenträger sicher gelöscht werden kann. Allerdings ist zu beachten, dass Festplatten und verschiedene Magnetbänder nach dem Löschen nicht mehr verwendet werden können, weil mit den aufgezeichneten Daten auch die Servospur, mit der der Schreib-/Lesekopf gesteuert wird, gelöscht wird. Das magnetische Löschen ist bei Verwendung geeigneter Löschgeräte sehr sicher, dennoch müssen Anwender bei der Bedienung Sorgfalt walten lassen, wenn das gewünschte Löschergebnis erzielt werden soll. Das gilt z. B. für die richtige Positionierung der Datenträger oder die Zeitdauer der Feldeinwirkung. Die Bedienungsanleitung der Löschgeräte ist in jedem Fall zu beachten. In der BSI-Publikation

		7500 zu Produkten für die materielle Sicherheit sind geeignete Löschgeräte aufgeführt. Ein Löschen von wiederbeschreibbaren CD-RWs, die nach dem magnetooptischen Verfahren arbeiten, ist mit den Löschgeräten nicht möglich, weil die Koerzitivfeldstärke dieser Datenträger zu groß ist. Ein alternatives Verfahren ist das Vernichten der Datenträger (siehe unten). Bei normalen Sicherheitsanforderungen sind beide Verfahren als gleichwertig anzusehen. • Komplettes Überschreiben Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der *komplette* Datenträger überschrieben wird. Die Überschreibprozedur sollte aus mindestens zwei, besser drei Durchläufen bestehen. Beim zweiten Durchlauf sollte das zum ersten Durchlauf komplementäre Datenmuster (Bit-Folge) verwendet werden. Für den dritten Durchlauf werden Zufallsdaten empfohlen. Dadurch wird eine verbesserte Schutzwirkung erzielt. Informationen in nicht unmittelbar zugreifbaren beschädigten Sektoren ("bad sectors") lassen sich nicht unmittelbar überschreiben und können unter Umständen wieder rekonstruiert werden. Schreibgeschützte oder nicht mehrfach beschreibbare Datenträger, wie CD-ROMs oder CD-Rs, können selbstverständlich auch nicht gelöscht werden und sollten vernichtet werden. • Überschreiben mit *VS-Clean* Um funktionstüchtige Festplatten (bis zum Geheimhaltungsgrad VS-VERTRAULICH) physikalisch zu löschen, stellt das BSI für die deutsche Bundesverwaltung die Software VS-Clean zur Verfügung. Datenträger mit einem höheren Geheimhaltungsgrad als VS-VERTRAULICH müssen zusätzlich - sofern sie nicht geeignet verschlüsselt sind - immer physisch vernichtet werden. Informationen über VS-Clean sind auf der Webseite des BSI unter "Produkte und Tools" zu finden. • Löschen von elektronischen Speichermedien RAM-Speicher (SRAM und DRAM) sind flüchtige Speicher, bei denen durch eine Trennung von der Stromversorgung der Speicherinhalt gelöscht wird. Eine Pufferbatterie, falls vorhanden, muss für die Löschung entfernt werden. Im Gegensatz dazu muss bei den nichtflüchtigen Speichern EEPROM und Flash-Memory zum Löschen des Speicherinhalts eine Spannung angelegt werden. Die korrekte Vorgehensweise ist den Datenblättern der Hersteller zu entnehmen. In beiden Fällen kann jedoch nicht ausgeschlossen werden, dass nach dem Löschen über "Spuren" in den Speicherzellen ein Rückschluss auf die vorher gespeicherten Daten möglich ist. Es wird deshalb empfohlen, den kompletten Speicher vor dem Löschen einmal mit Zufallszeichen vollständig zu überschreiben. • Vernichtung von Datenträgern Magnetische Datenträger wie Festplatten, die nicht mehr weiter verwendet werden sollen, können mit geeigneten Geräten vernichtet

		werden. Bei defekten Festplatten, die nicht mehr überschrieben werden können, bleibt als Löschverfahren nur das Vernichten der Festplatten. Die Vernichtung kann durch Shreddern erfolgen, aber auch thermische Verfahren wie Verbrennen oder Einschmelzen sind geeignet. Magnetbandkassetten können wie Festplattenlaufwerke mechanisch oder thermisch vernichtet werden. Das BSI hat für die Vernichtung von magnetischen Datenträgern mit Daten von hohem Schutzbedarf Partikelgrößen festgelegt. Für die Festplattenvernichtung wird eine Partikelgröße von maximal 300 Quadratmillimetern gefordert. Für die thermische Vernichtung wird eine Temperatur von circa 600°C bei einer Verweilzeit von mindestens 15 Minuten empfohlen. Aufgrund der Größe entsprechender Vernichtungsgeräte ist die Vernichtung bei Dienstleistungsfirmen in räumlicher Nähe sinnvoller als eine eigene Anschaffung der Geräte. Das Vernichtungsverfahren kann in Anlehnung an die Schrift BSI 7251 "Empfehlungen für die Vernichtung von Schlüsselgeräten" erfolgen, die im Bedarfsfall vom BSI zur Verfügung gestellt wird. Dienstleistungsfirmen, die eine Festplattenvernichtung anbieten, sind in der Produktliste BSI 7500 aufgeführt. Optische Datenträger, die nicht wiederbeschreibbar sind, können nicht gelöscht werden und müssen stattdessen mit geeigneten Geräten vernichtet werden, um die darauf gespeicherten Informationen sicher zu löschen. Wiederbeschreibbare Datenträger, beispielsweise CD-RWs, können grundsätzlich durch vollständiges Überschreiben gelöscht werden. Es ist jedoch nicht bekannt, ob Spuren der alten Informationen verbleiben und rekonstruiert werden können. Bei erhöhtem Schutzbedarf müssen deshalb auch wiederbeschreibbare Datenträger mit geeigneten Geräten vernichtet werden, um die darauf gespeicherten Informationen sicher zu löschen. Für die Vernichtung von optischen Datenträgern wie CDs oder DVDs wird eine Partikelgröße von maximal 10 Quadratmillimetern bei hohem oder sehr hohem Schutzbedarf und von maximal 200 Quadratmillimetern bei normalem Schutzbedarf gefordert. In der Produktliste BSI 7500 sind geeignete Vernichtungsgeräte aufgeführt. Alternativ können auch thermische Vernichtungsverfahren, z. B. Einschmelzen, angewandt werden. Die BSI-Publikation 7500 listet zwar Vernichtungsgeräte für Disketten und CDs auf, Geräte für die schreibtischnahe Vernichtung von Magnetbandkassetten sind derzeit jedoch nicht bekannt. Magnetbandkassetten können deshalb nur in Großgeräten (z. B. Schneidmühlen) oder thermisch (Verbrennen, Einschmelzen) vernichtet werden.
M 4.234	(B)	**Aussondern von IT-Systemen** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator, Benutzer IT-Systeme sind dem ständigen Wandel der Technik unterworfen.

		Daher werden sie häufiger ausgetauscht als viele andere Arbeitsmaterialien. Da sich auf IT-Systemen aber schutzbedürftige Daten und Anwendungen befinden können, ist die Weitergabe oder Aussonderung von IT-Systemen zu regeln. Unabhängig davon, ob ausrangierte IT-Systeme an andere Abteilungen weitergegeben werden, an Mitarbeiter verschenkt, verkauft oder verschrottet werden, muss sichergestellt sein, dass alle Daten und Anwendungen vorher sorgfältig gelöscht wurden (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*). Vorher ist zu überprüfen, ob die Daten gesichert wurden, soweit sie noch benötigt werden. Es empfiehlt sich, dass beide Schritte vom jeweils Zuständigen schriftlich bestätigt werden.

2.3.6 Notfallvorsorge

M 6.91 *	(C)	**Datensicherung und Recovery bei Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator Auch Loadbalancer sollten in das übergeordnete Datensicherungskonzept einbezogen werden. Dabei kommt insbesondere der Sicherung der Konfigurationsdateien eine hohe Bedeutung zu. Da im Rahmen einer zentralen Administration Konfigurationsdateien oftmals auf separaten Servern gehalten und auch von dort geladen werden, kann auch die Sicherung über diese Server erfolgen. Die Konfigurationsdateien auf diesen Servern sind vor unberechtigtem Zugang zu schützen. Dies gilt insbesondere dann, wenn in den Konfigurationsdateien Passwörter im Klartext gespeichert sind. Falls zur Sicherung der Konfigurationsdateien ein TFTP-Server eingesetzt wird, so darf dieser nur im Administrationsnetz erreichbar sein. Alternativ kann bei einigen Systemen eine Datensicherung auch über die Verwendung von PCMCIA-Speichereinschüben erfolgen. Um auf die Nutzung der Datensicherung vorbereitet zu sein, müssen regelmäßig Recovery-Übungen zum Wiederherstellen der Sicherung durchgeführt werden (siehe hierzu auch M 6.41 Übungen zur Datenrekonstruktion). Weiterführende Maßnahmen:

		• M 6.36 Festlegung des Minimaldatensicherungskonzeptes • M 6.37 Dokumentation der Datensicherung • M 6.35 Festlegung der Verfahrensweise für die Datensicherung • M 6.41 Übungen zur Datenrekonstruktion
M 6.92 *	(C)	**Notfallvorsorge bei Loadbalancer** Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Administrator <u>Fehlerbehandlung bei Loadbalancer</u> In jedem IT-Betrieb treten Störungen auf, die von sporadisch auftretenden Fehlverhalten von Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts und dadurch verursachten Netzausfällen reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software beispielsweise auf Grund von Defekten oder Kompromittierungen. Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien und als Ergebnis von bereits aufgetretenen Störungen sollten Handlungsanweisungen erstellt werden. Kochbuchartige Dokumentationen aller notwendigen Kommandos, ihrer Anwendung mit den zu erwartenden Ausgaben sind in Situationen, die schnelles Handeln erfordern, besonders hilfreich. Hierzu gehören neben Diagnose und Fehlerbehandlung auch die im normalen Betrieb notwendigen Administrationstätigkeiten. Letztere können typischerweise bereits in der vom Hersteller gelieferten Dokumentation enthalten sein. Für die tägliche Praxis ist es allerdings sinnvoll, eine Gesamtdokumentation in Form eines Betriebshandbuchs zu erstellen. Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört auch eine geeignete Protokollierung während des Betriebs (siehe auch M 4.205* Protokollierung bei Loadbalancern). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden. Dazu existieren sowohl frei verfügbare als auch kommerzielle Programme, oft auch vom Hersteller der Geräte. Die Verwendung geeigneter Werkzeuge ist umso wichtiger, da mit den Systemkommandos nicht immer alle Konfigurationseinstellungen angezeigt werden. Teilweise werden lediglich die von den Standardeinstellungen abweichenden

		Daten erfasst.
		
		Die Vorgehensweise bei der Fehlerbehandlung lässt sich in die Bereiche Administration, Performancemessung und Diagnose unterteilen. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt:
		
		<u>Administration</u>
		
		In einem Betriebshandbuch sollten alle notwendigen Kommandos zu Administration und Konfiguration dokumentiert werden.
		
		Folgende Bereiche sind zu berücksichtigen:
		• Einrichten von Accounts
		• Update des Betriebssystems
		• Konfiguration
		  ○ Interface
		  ○ Line-Ports
		  ○ Reale und Virtuelle Server
		  ○ Lastverteilte Dienste und deren Parameter
		  ○ Access-Control-Lists
		  ○ Routing
		• Protokollierung
		
		<u>Performance</u>
		
		Folgende Aspekte sollten für Aussagen über die Performance berücksichtigt werden:
		• Eingehender und ausgehender Verkehr (pro Interface oder Port)
		• Durchsatz oder Verkehr pro Interface
		• Statistikinformationen pro Virtuellem Server
		• Statistikinformationen pro Realem Server
		• Statistikinformationen der verwendeten Protokolle
		• Statistikinformationen der lastverteilten Dienste
		
		<u>Diagnose</u>
		
		Für die Diagnose sollten alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige der Zustände des Gesamtsystems, der Interfaces und ihrer Konfiguration dokumentiert sein. Viele Kommandos ermöglichen zudem einen Debug-Modus zu Ausgabe

		umfangreicher Statusinformationen. Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant: • Status der Netz-Interfaces und der sonstigen Anschlüsse • Status der TCP- und UDP-Netzdienste • Gesamtkonfiguration als Überblick • Prozesse • Sitzungstabelle • Statusabfrage der konfigurierten Virtuellen und Realen Server, Interpretation des Healthchecks • Routing Tabelle und genutzte Routing Protokolle • ARP-Tabelle • Protokollierung (Interpretation der Log-Informationen) Als weiterführende Maßnahmen sollte M 2.215 Fehlerbehandlung betrachet werden. <u>Notfallvorsorge zur Steigerung der Verfügbarkeit</u> Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 Notfallvorsorge-Konzept). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen bez. Aufbau, Inhalt und Form fest. Folgende Fragestellungen sind für die Notfallvorsorge relevant: • Welche Anforderungen bestehen an das Monitoring? • Zusammenstellung der Informationen, die von den für den Betrieb der Netzkomponenten verantwortlichen Stellen immer ausgewertet werden (siehe auch Abschnitt Protokollierung) o Wie kann eine frühzeitige Störungserkennung sicher gestellt werden? • Was sind Gründe für mögliche Störungen? o Hardware-Defekte o Zu geringe Dimensionierung (Ausfall bei Steigerung der Last)

		• Welche Vorsorgemaßnahmen können getroffen werden?
		  ○ Ersatzgeräte
		  ○ Ersatzteile
		  ○ Implementierung von Failover-Lösungen, die im laufenden Betrieb ein
		  ○ Umschalten auf ein Alternativgerät ermöglichen
		  ○ Wartungsverträge
		  ○ Ausbildung der Mitarbeiter
		• Welche Service Level Agreements bestehen oder sollten getroffen werden?
		  ○ Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten)
		  ○ Interne Service Level Anforderungen
		• Wie ist eine Diagnose durchzuführen?
		  ○ Statusabfragen
		  ○ Anzeige der Konfiguration
		  ○ Prozesse
		  ○ Routing
		  ○ Angemeldete Nutzer
		  ○ Protokollierung
		• Welche Entstörprozeduren müssen durchgeführt werden?
		  ○ Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von
		  ○ Betriebssystem und Konfiguration)
		  ○ Vorgehen bei Ausfall von Teilkomponenten, bspw. Speicher
		• Wer ist im Schadensfall zu benachrichtigen?
		  ○ Server- und Anwendungsadministration
		  ○ Hardware-Lieferant/Ansprechpartner für den Wartungsvertrag
		• Welche Dokumente müssen im Schadensfall verfügbar sein?
		  ○ Konfiguration

		○ ACLs (Regelwerk) ○ Eingerichtete Nutzer und Berechtigungen ○ Passwörter Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROMs oder anderen Datenträgern gesondert hinterlegt werden. • Wie verläuft der Wiederanlauf? ○ Abhängigkeiten zu anderen Netzkomponenten bzw. Bereichen des IT-Verbunds ○ Neuinstallation des Betriebssystems und Konfiguration ○ Zurückspielen einer gesicherten Konfiguration ○ Möglichkeiten eines eingeschränkten Betriebs Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Gerätetypen und Betriebssystemen berücksichtigt werden. Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist die Vorhaltung von Ersatzteilen, um bei Hardware-Defekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

3 Kreuzreferenztabellen

Nachfolgende Tabelle listet die im Baustein Loadbalancer enthaltenen Sicherheitsmaßnahmen auf und stellt diese denjenigen Gefährdungen gegenüber, gegen welche die einzelnen Maßnahmen wirken:

	Siegel	G 1. 2*	G 2. 1*	G 2. 3*	G 2. 4	G 2. 22*	G 2. 27*	G 2. 44*	G 2. 54	G 2. 98*	G 3. 64*	G 3. 65*	G 4. 22*	G 4. 49*	G 5. 4	G 5. 28	G 5. 112	G 5. 113	G 5. 114*	G 5. 115	G 9. 10
M 1.43	A														X						
M 2.35	B												X								
M 2.167	B								X												
M 2.273	A												X								
M 2.278*	Z									X											
M 2.279*	A		X																		
M 2.280*	C			X				X		X											
M 2.281*	A						X														
M 2.282*	A				X																
M 2.283*	B												X								
M 2.302*	Z															X					
M 2.314*	Z	X																			
M 3.38*	B										X	X									
M 4.201*	A										X			X							
M 4.202*	A										X			X			X	X			
M 4.203*	A										X			X					X	X	X
M 4.204*	C																X		X	X	X
M 4.205*	C					X															X
M 4.234	B								X												
M 5.70*	A															X					
M 5.111*	C										X										
M 6.91*	C											X									
M 6.92*	C											X									